

STATE OF MICHIGAN
DEPARTMENT OF MANAGEMENT AND BUDGET
PURCHASING OPERATIONS
P.O. BOX 30026, LANSING, MI 48909
OR
530 W. ALLEGAN, LANSING, MI 48933

December 4, 2007

CHANGE NOTICE NO. 6
TO
CONTRACT NO. 071B3001210
between
THE STATE OF MICHIGAN
and

NAME & ADDRESS OF VENDOR		TELEPHONE (512) 495-9487 Andrew Trickett
Global Secure Systems Corporation P.O. Box 2985 LA Jolla, CA 92038 Andrew.trickett@virtualalert.com		VENDOR NUMBER/MAIL CODE
		BUYER/CA (517) 241-7233 Joann Klasko
Contract Compliance Inspector: Karen McMaster: (517) 335-8150 Health Alert Network (HAN) for Department of Community Health		
CONTRACT PERIOD: From: March 17, 2003 To: September 30, 2012		
TERMS N/A	SHIPMENT N/A	
F.O.B. N/A	SHIPPED FROM N/A	
MINIMUM DELIVERY REQUIREMENTS N/A		

NATURE OF CHANGE (S):

Effective immediately, this contract is hereby **EXTENDED** to September 30, 2012 and **INCREASED** by \$1,600,000.00 for services. Please see attached revised proposal from the vendor dated 11/09/2007. Please note that the buyer has been changed to Joann Klasko.

All other terms and conditions remain the same.

AUTHORITY/REASON:

Per agency request and vendor approval and State Administrative Board approved \$500,000.00 on 9/11/2007 and \$1,100,000.00 on 10/16/2007.

INCREASE: \$1,600,000.00

TOTAL REVISED CONTRACT VALUE: \$4,852,666.70



GLOBALSECURE SYSTEMS™

ONE FOCUS. ONE RESULT.

November 9, 2007

Sara Williams
Contract Liaison
DIT DLEG/DCH Agency Services
Lansing, MI
Via Email

Dear Sara,

Regarding the extension of the existing contract, Global Secure Systems (GSS) is willing to work under the same contract terms and conditions for the period covering October 1, 2007 through September 30, 2010.

I am pleased to submit a quote for maintenance coverage and hosting services on Response Manager and Volunteer Mobilizer, currently in use by the Department of Community Health. DCH is licensed for one instance of Response Manager – Primary, one instance of Response Manager – Backup, one instance of Volunteer Mobilizer – Primary and one instance of Volunteer Mobilizer – Backup. The following table defines the annual maintenance cost associated with each instance.

Maintenance Fees

<u>Description</u>	<u>Total</u>
Response Manager Primary System Maintenance	\$59,910.00
Response Manager Backup System Maintenance	\$59,910.00
Volunteer Mobilizer Primary System Maintenance	\$15,000.00
Volunteer Mobilizer Backup System Maintenance	\$7,500.00
Total	\$142,320.00

The following table defines the annual hosting cost associated with each instance, the phone circuit costs and estimated phone charges.

Hosting Fees

<u>Description</u>	<u>Total</u>
Response Manager Primary System Hosting	\$91,200.00
Response Manager Backup System Hosting	\$91,200.00
Volunteer Mobilizer Primary System Hosting	\$15,000.00
Volunteer Mobilizer Backup System Hosting	\$15,000.00
Primary PRI Phone Circuit	\$6,660.00
Backup PRI Phone Circuit	\$6,660.00
Total	\$225,720.00

Headquarters:

8601 RR 2222 BUILDING 1 STE. 290
AUSTIN, TEXAS 78730
512.342.6330 OFFICE
512.342.2449 FAX

5112 ARNOLD AVENUE
MCCELLELLAN, CALIFORNIA 95652
916.640.1600 OFFICE
916.640.1473 FAX

1033 N. FAIRFAX ST. SUITE 302
ALEXANDRIA, VIRGINIA 22314
703.548.5191 OFFICE
703.548.5193 FAX

systems@globalsecurecorp.com
WWW.GLOBALSECURECORP.COM



Estimated Phone Charges

<u>Description</u>	<u>Total</u>
Annual	\$24,000.00

The final table defines miscellaneous maintenance costs that should be planned for on an annual basis.

Miscellaneous Maintenance Costs

<u>Description</u>	<u>Total</u>
Hardware Refresh	\$30,960.00
Software Refresh	\$45,000.00
Misc. Component Refresh	\$15,000.00
Feature Acceleration	\$50,000.00
Total	\$140,960.00

3 Year Totals

Maintenance Fees	\$142,320.00 x 3 years = \$426,960.00
Hosting Fees	\$225,720.00 x 3 years = \$677,160.00
Estimated Phone Charges	\$ 24,000.00 x 3 years = \$ 72,000.00
Misc. Maintenance Costs	\$140,960.00 x 3 years = \$422,880.00

Grand Total	\$1,599,000.00
--------------------	-----------------------

If you have any questions, please contact your Account Manager, Dan Smith at 410-472-9005 or email at dsmith@globalsecurecorp.com. We appreciate your business.

Sincerely,

Andrew F. Trickett
Vice President
Global Secure Systems

cc: Dan Smith
Bill Colville
Brook Babcock
Pete Coscarelli
Linda Myers
Sheryl Conway
Marsha Teichman

STATE OF MICHIGAN
DEPARTMENT OF MANAGEMENT AND BUDGET
PURCHASING OPERATIONS
P.O. BOX 30026, LANSING, MI 48909
OR
530 W. ALLEGAN, LANSING, MI 48933

February 21, 2007

CHANGE NOTICE NO. 5 (REVISED)
TO
CONTRACT NO. 071B3001210
between
THE STATE OF MICHIGAN
and

NAME & ADDRESS OF VENDOR		TELEPHONE (512) 495-9487 Andrew Trickett
Global Secure Systems Corporation P.O. Box 2985 LA Jolla, CA 92038 Andrew.trickett@virtualalert.com		VENDOR NUMBER/MAIL CODE
		BUYER/CA (517) 335-4804 Douglas Collier
Contract Compliance Inspector: Karen McMaster: (517) 335-8150 Health Alert Network (HAN) for Department of Community Health		
CONTRACT PERIOD: From: March 17, 2003		To: September 30, 2007
TERMS N/A	SHIPMENT N/A	
F.O.B. N/A	SHIPPED FROM N/A	
MINIMUM DELIVERY REQUIREMENTS N/A		

NATURE OF CHANGE (S):

Effective immediately, this contract is hereby **EXTENDED** to September 30, 2007 and **INCREASED** by \$392,040.00 for services. Please see attached revised proposal from the vendor dated 11/14/2006. Please note that the buyer has been changed to Douglas Collier.

All other terms and conditions remain the same.

AUTHORITY/REASON:

Per agency request and vendor approval.

INCREASE: \$392,040.00

TOTAL REVISED CONTRACT VALUE: \$3,252,666.70

STATE OF MICHIGAN
DEPARTMENT OF MANAGEMENT AND BUDGET
PURCHASING OPERATIONS
P.O. BOX 30026, LANSING, MI 48909
OR
530 W. ALLEGAN, LANSING, MI 48933

February 7, 2007

CHANGE NOTICE NO. 5
TO
CONTRACT NO. 071B3001210
between
THE STATE OF MICHIGAN
and

NAME & ADDRESS OF VENDOR		TELEPHONE (512) 495-9487 Andrew Trickett
Global Secure Systems Corporation P.O. Box 2985 LA Jolla, CA 92038 Andrew.trickett@virtualalert.com		VENDOR NUMBER/MAIL CODE
		BUYER/CA (517) 335-4804 Douglas Collier
Contract Compliance Inspector: Karen McMaster: (517) 335-8150 Health Alert Network (HAN) for Department of Community Health		
CONTRACT PERIOD: From: March 17, 2003		To: September 30, 2007
TERMS N/A	SHIPMENT N/A	
F.O.B. N/A	SHIPPED FROM N/A	
MINIMUM DELIVERY REQUIREMENTS N/A		

NATURE OF CHANGE (S):

Effective immediately, this contract is hereby **EXTENDED** to September 30, 2007 and **INCREASED** by \$392,040.00 for services. Please see attached revised proposal from the vendor dated 11/14/2006. Please note that the buyer has been changed to Douglas Collier.

All other terms and conditions remain the same.

AUTHORITY/REASON:

Per agency request and vendor approval.

TOTAL ESTIMATED CONTRACT VALUE REMAINS: \$2,860,626.70



Revised Proposal dated October 9, 2006: ITN DOH 15-10
GLOBAL SECURE SYSTEMS™
ONE FOLLOW ONE RESULT

November 14, 2006

Mr. William Cobille
Michigan Department of Community Health
1001 Terminal Road
Lansing, MI 48906

RE: Contract Renewal

Mr. Cobille,

Regarding the extension of the existing contract, Global Secure Systems (GSS) is willing to work under the same contract terms and conditions for the period covering October 1, 2006 through September 30, 2007.

Best regards,

Via Email

Andrew F. Trickert
Vice President
Global Secure Systems

THIS CRANK REPLACES

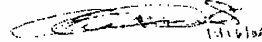
PREVIOUS DIT ORDER

ANT #196 020

CRS # 20071272.00

FULL YEAR CONTRACT

ATTACHED


11/14/06

HOMELAND SECURITY
100% FEDERAL FUNDS

Hosting Fees Oct 06 - Mar 07

<u>Model</u>	<u>Description</u>	<u>Quantity</u>	<u>Unit Price</u>	<u>Total</u>
GSS	Primary System Hosting	12	\$ 8,850.00	\$ 106,200.00
GSS	Backup System Hosting	12	\$ 8,850.00	\$ 106,200.00
GSS	Primary PRI	12	\$ 555.00	\$ 6,660.00
GSS	Backup PRI	12	\$ 555.00	\$ 6,660.00
	Total			\$ 225,720.00

Maintenance Fees

<u>Model</u>	<u>Description</u>	<u>Quantity</u>	<u>Unit Price</u>	<u>Total</u>
GSS	RM Primary System Maint.	12	\$ 4,992.50	\$ 59,910.00
GSS	RM Backup System Maint.	12	\$ 4,992.50	\$ 59,910.00
GSS	VM Primary System Maint.	12	\$ 1,250.00	\$ 15,000.00
	Total			\$ 134,820.00

Volunteer Mobilizer Backup Site

<u>Model</u>	<u>Description</u>	<u>Quantity</u>	<u>Unit Price</u>	<u>Extended</u>
GSS	Maint	12	\$ 625.00	\$ 7,500.00

Estimated Phone Charges

<u>Model</u>	<u>Description</u>	<u>Quantity</u>	<u>Unit Price</u>	<u>Total</u>
GSS	Monthly Oct06-Mar07	12	\$ 2,000.00	\$ 24,000.00

Total 12 Mos. Projections (Oct 06 - Mar 07) \$ 392,040.00

HOMELAND SECURITY
100% FEDERAL FUNDS

STATE OF MICHIGAN
DEPARTMENT OF MANAGEMENT AND BUDGET
ACQUISITION SERVICES
P.O. BOX 30026, LANSING, MI 48909
OR
530 W. ALLEGAN, LANSING, MI 48933

October 30, 2006

CHANGE NOTICE NO. 4
TO
CONTRACT NO. 071B3001210
between
THE STATE OF MICHIGAN
and

NAME & ADDRESS OF VENDOR		TELEPHONE (512) 495-9487 Andrew Trickett
Global Secure Systems Corporation P.O. Box 2985 LA Jolla, CA 92038 Andrew.trickett@virtualalert.com		VENDOR NUMBER/MAIL CODE
		BUYER/CA (517) 373-7396 Andy Ghosh
Contract Compliance Inspector: Karen McMaster: (517) 335-8150 Health Alert Network (HAN) for Department of Community Health		
CONTRACT PERIOD: From: March 17, 2003 To: December 31, 2006		
TERMS N/A	SHIPMENT N/A	
F.O.B. N/A	SHIPPED FROM N/A	
MINIMUM DELIVERY REQUIREMENTS N/A		

NATURE OF CHANGE (S):

Effective immediately, this contract is hereby EXTENDED through December 31, 2006. Also, this contract is hereby UPDATED to reflect a name change to Global Secure Systems Corporation from Virtual Alert Inc.

All other terms and conditions remain the same.

AUTHORITY/REASON:

Per agency request and vendor approval.

TOTAL ESTIMATED CONTRACT VALUE REMAINS: \$2,860,626.70

STATE OF MICHIGAN
DEPARTMENT OF MANAGEMENT AND BUDGET
ACQUISITION SERVICES
P.O. BOX 30026, LANSING, MI 48909
OR
530 W. ALLEGAN, LANSING, MI 48933

July 8, 2004

CHANGE NOTICE NO. 3
TO
CONTRACT NO. 071B3001210
between
THE STATE OF MICHIGAN
and

NAME & ADDRESS OF VENDOR	TELEPHONE (512) 495-9487 Andrew Trickett
Virtual Alert Inc. P.O. Box 2985 LA Jolla, CA 92038 Andrew.trickett@virtualalert.com	VENDOR NUMBER/MAIL CODE
	BUYER/CA (517) 373-7396 Andy Ghosh
Contract Compliance Inspector: Karen McMaster: (517) 335-8150 Health Alert Network (HAN) for Department of Community Health	
CONTRACT PERIOD: From: March 17, 2003 To: September 30, 2006	
TERMS N/A	SHIPMENT N/A
F.O.B. N/A	SHIPPED FROM N/A
MINIMUM DELIVERY REQUIREMENTS	
N/A	

NATURE OF CHANGE (S):

Effective immediately, this contract is hereby EXTENDED through September 30, 2006. Also, this contract is hereby INCREASED by \$1,643,691.00.

See the attached proposal from the contractor.

All other terms and conditions remain the same.

AUTHORITY/REASON:

Per agency request (Sara Williams) and approval per Virtual Alert, Inc.

INCREASE: \$1,643,691.00

TOTAL REVISED ESTIMATED CONTRACT VALUE: \$2,860,626.70

License Type	Original Base	Original Option	Original Upside	Calculated Match Base	Calculated Match Upside
Level 4 User CALs	481	150	631	543	837
Level 2+ User CALs	1,386	1,070	2,456	1,564	3,257
Total Users	1,867	1,220	3,087	2,107	4,094
Server Systems	2		primary production site + backup site No extra MISA, directory, etc. servers within individual set up.		
Redundancy Requirements on specific items	none				
Scenario (1 = exercise option for more CALs)	1	Exercise Option			
Number of months	24				

Pricing Granted			
Level 4 Users	837	\$ 495.00	\$ 414,259.62
Level 2+ Users	3,257	\$ 120.00	\$ 390,883.78
BTRS Server - Production Site	1	\$145,200.00	\$ 145,200.00
BTRS Server - Backup Site	1	\$ 45,000.00	\$ 45,000.00
Communications Servers	2	\$ 35,000.00	\$ 70,000.00
PRE-DISCOUNT SUBTOTAL			\$ 1,065,343.41
Discount on User and BTRS Licenses	20%	\$	(199,068.68)
POST-DISCOUNT SUBTOTAL		\$	866,274.73
Annual Maintenance	24 months @ 18% per annum	\$	383,519.63
VA SOFTWARE TOTAL		\$	1,249,794.35
Installation	2	\$ 14,730.00	\$ 29,460.00

Standard Pricing			
Level 4 Users	837	\$ 495.00	\$ 414,259.62
Level 2+ Users	3,257	\$ 120.00	\$ 390,883.78
BTRS Server - Production Site	1	\$ 145,200.00	\$ 145,200.00
BTRS Server - Backup Site	1	\$ 45,000.00	\$ 45,000.00
Communications Servers	2	\$ 38,000.00	\$ 76,000.00
PRE-DISCOUNT SUBTOTAL			\$ 1,071,343.41
Discount on User and BTRS Licenses	0%	\$	-
POST-DISCOUNT SUBTOTAL			\$ 1,071,343.41
Annual Maintenance	30% per annum	\$	642,802.04
VA SOFTWARE TOTAL		\$	1,714,145.45
Installation	2	\$ 19,000.00	\$ 38,000.00

Manually
adjusted
maint to
hit a
target #

						Does not include travel costs using FTR. 8k for travel estimate						
Pre-Installation Consultation	1	\$	42,600.00	\$	42,600.00		1	\$	49,000.00	\$	49,000.00	
Co-location Set-up Fee	2	\$	3,000.00	\$	6,000.00		2	\$	3,000.00	\$	6,000.00	
Training - 5 day package	1	\$	10,000.00	\$	10,000.00		1	\$	10,000.00	\$	10,000.00	
ONE-TIME PROF SVCS				\$	88,060.00					\$	103,000.00	
Monthly Operations per Server	2	24	\$	6,850.00	\$	328,800.00		24	\$	6,850.00	\$	328,800.00
TOTAL VA SERVICES				\$	416,860.00					\$	431,800.00	
Technical Service Desk with Maint	80		\$	-	\$	-		80	\$	150.00	\$	12,000.00
vaVolunteer Module	1	\$	50,000.00	\$	50,000.00		1	\$	75,000.00	\$	75,000.00	
Maintenance	30%			\$	15,000.00				30%	\$	22,500.00	
Total for vaVolunteer				\$	65,000.00					\$	97,500.00	
TOTAL				\$	1,731,654.35		TOTAL			\$	2,255,445.45	

Price Diffence -- dollars	\$ (523,791.10)
Price Diffence -- percent	-23%



April 14, 2004

Sara Williams, Contract Administrator
Michigan Department of Information Technology
Chandler Plaza
300 East Michigan Avenue
Lansing MI 48913

Dear Ms. Williams,

Virtual Alert is very pleased to provide this proposal for extension of Contract No. 071B3001210 between Virtual Alert and the State of Michigan. This proposal intends to present renewal of existing arrangements, enhancements that the State of Michigan has indicated that it definitely intends to pursue, as well as options that it has indicated that it may or may not pursue. We will endeavor to clarify which line items fall within each category, on an item-by-item basis.

We will also make clear which items are firm price quotes from Virtual Alert, which are estimates for Virtual Alert services, and which are third-party components for which we are providing non-binding estimates only for the convenience of the State of Michigan to aid in its comprehensive budgeting work.

Virtual Alert understands that the price, scope, definitions and terms and conditions not specifically addressed in this proposal will be based on our existing contract. In case items in this proposal are in direct conflict with our existing contract, the existing contract will take precedence.

We look forward to the continuation and enhancement of an already mutually beneficial relationship.

Best regards,

Andrew F. Trickett
Executive Director

Copy: Mr. Bill Colville, the State of Michigan
Ms. Karen MacMaster, the State of Michigan
Ms. Linda Myers, MDIT

1. GENERAL AND GLOBAL PARAMETERS AND LIMITATIONS

As indicated in the introductory letter, this proposal goes beyond the provision of firm fixed prices. The State of Michigan and Virtual Alert have discussed a number of options and enhancements to the Michigan Health Alert Network. Virtual Alert recognizes the need for the State of Michigan to have summary estimates of total costs. Virtual Alert is providing summary estimates of its services and of the estimated cost of third party hardware and software components. Except where stated, these are not binding. But Virtual Alert has provided not-to-exceed cost estimates in good faith for the each of the options presented herein. Virtual Alert understands the State of Michigan may elect to procure third-party hardware and software components from alternative contractors. For both parties' protection, no option will be initiated until detailed requirements have been specified and agreement has been achieved between the two parties.

Virtual Alert is providing a quote for the State of Michigan to utilize BTRS primarily for public health officials for the CDC Bioterrorism Grant program. This philosophy applies especially to server licenses. Virtual Alert is going to be very reasonable in acknowledging that response to bioterrorism involves officials from homeland security, public safety / law enforcement, emergency management agencies, EMS, etc. However, Virtual Alert reserves the right to define additional servers/systems as essentially "new clients", for which the "subsequent license" discounts for server licenses will not apply. The purpose is not to impose unreasonable restrictions. Rather, the purpose is to ensure that Virtual Alert is not being, de facto, forced to support additional, completely different "systems" than the one that has been purchased.

For all professional services quotes, these do not include travel and materials expenses, which will be billed, at cost. For all hourly rates, prices will escalate by 5% per contract year starting October 1, 2005.

2. BTRS USER LICENSE DEFINITIONS

Client access licenses (CALs) are priced on a per-user basis, which vary depending upon the type of user and the functionality they are allowed to utilize. Virtual Alert will not charge the State of Michigan incremental user CALs for backup/hot or test environment sites utilized primarily by the State of Michigan.

Translations from the Original Contract

All CALs previously purchased as "Level 4" licenses will be converted, at no additional cost, to "Administrator" licenses. The below table will show that there is no degradation in functional rights for such users.

All CALs previously purchased as "Level 2+" licenses will be converted, at no additional cost, to "Collaborator" licenses. The below table will show that there is actually an increase in functional rights for such users. Virtual Alert will continue to honor the original pricing table for Level 2+ licenses to apply to Collaborator licenses.

Pricing Structure

- Virtual Alert will continue to honor the original pricing table for Level 4 licenses to apply to Administrator licenses and for Level 2+ licenses to apply to Collaborator licenses
- The State of Michigan may purchase the newly created "Alert Only" Licenses (no comparable level in original contract) at a rate equal to one-sixth the cost of "Collaborator" (i.e., \$20 per license list price). "Alert Only" Licenses will have the functionality rights shown in the following chart
- The State of Michigan may purchase "Directory Only" Licenses (no comparable level in original contract) at a rate equal to one-half the cost of "Alert Only" (i.e., \$10 per license list price). "Directory Only" license users may only utilize the role-based authentication model provided in BTRS - no portal or alerting send/receipt

Functionality Rights Summary Table

	<u>Administrator License</u>	<u>Collaboration License</u>	<u>Alert-Only License</u>	<u>Directory-Only License</u>
<u>Major Functionality Areas</u>				
Administer Other Users	√			
Administer Roles	√			
Administer Groups	√			
Administer Folders	√			
Access to Collaboration Tools (1)	√	√		
Can Send Alerts	√	√		
Access to Read-only Information (2)	√	√	√	
Can Self-Administer Profile Info (3)	√	√	√	
Can Receive Alerts	√	√	√	
Can Authenticate Through Directory (4)	√	√	√	√
(1) Discussions, as well as check-in/check-out, draft/publish, fax/email distribute documents				
(2) Can see posted information and download documents on "semi-public" sites				
(3) Can self-maintain contact data, password/PIN, and alerting profiles				
(4) Whether for BTRS or for other applications				

Proposed User Re-configuration

The State of Michigan has requested that it be able to re-configure the number and types of user CALs from its original purchase of Level 4/Administrator and Level 2+/Collaborator licenses (as set forth below). Virtual Alert has agreed to such a one-time swap, as long as total license and maintenance dollars due to Virtual Alert (according to the pricing structure set forth above) is the same. Virtual Alert accepts the State of Michigan's proposed re-configuration which is set forth in the table below:

<u>Previous Arrangment</u>	<u>Number</u>	<u>Requested</u>	<u>Number</u>
Level 4	481	Admin	250
Level 2+	1386	Collaborator	2110
		Alert-only	1000
		Directory Only	0
Total	1867	Total	3360
Virtual Alert will accept this reconfiguration			

Gratis CALS

The State of Michigan maintains the ability to request free user licenses from Virtual Alert, in order to add small numbers of individuals from jurisdictions outside of Michigan. Virtual Alert retains the right to set the number and definition for users eligible for such licenses.

3. BTRS SERVER LICENSE DEFINITIONS

The server license for BTRS is priced on a per-server-installed basis. The State of Michigan will need to purchase at least one (1) server license in order to use BTRS, which it has already done in the original contract. In order to use BTRS on backup/hot sites and test/training environments, Virtual Alert provides very significant discounts for subsequent server license purchases. This arrangement holds true only for an individual "client". Virtual Alert reserves the right to interpret whether a subsequent server license is for the same "client" or a new one. The list pricing for primary production server licenses is \$145,000.

Backup sites and test/training environments as defined as exact replicas of the primary production site. The list price for such sites is \$45,000. The State of Michigan currently owns one such site.

Separate workspace sites are defined as installations in which a new SharePoint portal (different home page, different document library) is being utilized, but the original directory and alert infrastructure is being utilized. The MIHAN system currently does not have such a site. The list price for such sites is \$75,000, which covers all primary production sites and backup/test sites for which the "main" MIHAN system exists.

The State of Michigan has the option to purchase independent instances of vaMessenger for a list price of \$30,000. There are no Virtual Alert software fees involved in merely adding more bandwidth to the existing

alerting infrastructure. A separate instance is involved only if the State of Michigan wanted to establish vaMessenger alerting infrastructure that operates independently from the existing infrastructure.

All server licenses are one-time costs. For all of these BTRS Server License options, discounting will apply according to schedule set forth for CAL threshold discount levels. Therefore, the actual discount will depend upon where the State of Michigan happens to lie in the CAL threshold schedule at time of purchase of the particular server license.

Additional backup, test, training and extra portal sites are subject to a \$5000 install fee per site. This fee level assumes that Virtual Alert is still managing the system in the co-location arrangement.

4. BASELINE SOFTWARE MAINTENANCE

The original contract produced a license base of \$664,615.00. There were no additions to the license base since the original contract, nor are any expected before this renewal commences. Therefore, the license base is still at that original amount. The maintenance rate will stay at 18% annually and will be due up front and in full. Therefore, the amount due at renewal is \$119,630.70

Any additions to the license base, at any time during the period of the extended contract, are subject to the same maintenance rate, up front and in full. Virtual Alert is willing to allow the State of Michigan (or any other purchasing entity) to pay a pro-rated amount, so that the timing of the maintenance renewal for any additions will match that of the original \$119,630.70 license base.

The 18% maintenance rate will not escalate for the term of this contract renewal. If the State of Michigan purchases maintenance amounts that cover more than one year in advance, it will enjoy a 5% discount on such "out year" purchases. For instance, if it purchases 2 years of maintenance on Sept. 1, 2004, it will pay the normal amount for the period covering 10/1/04 – 9/30/05 and enjoy a 5% discount for the period covering 10/1/05 – 9/30/06.

The original BTRS Software Maintenance agreement is the governing document for the contractual arrangements for this maintenance. The one exception to that statement is that the State of Michigan will now enjoy 80 free hours per contract year of custom work. Such work is generally scoped to include: work done for support requests that are later found to have not been caused by BTRS; minor technical customizations; research for potential custom work; generation of special reports; direct support for end users.

5. Developer and Functional Management Support

The State of Michigan may submit work orders to Virtual Alert to provide developer and functional management support to the State of Michigan. Such work could include technical customizations, support for 3rd party developers leveraging the BTRS platform (i.e., for the APIs) and generation of reports that require technical staff to execute, assistance in planning, executing and assessing formal exercises or business rules assistance for new entities that join MIHAN. Under no circumstances will any work be independently initiated by Virtual Alert. The State of Michigan must initiate all work orders and no work will begin until written authorization from the State of Michigan after both parties achieve agreement regarding the work order scope and cost.

The total developer and functional management support budget will not exceed \$110,000 using a combination of the following labor rates.

- Program Manager - \$150/hour
- Project Manager - \$145/hour
- Integration Technician - \$120/hour
- Developer Support - \$100/hour
- These rates will escalate at 5% per year starting October 1, 2005.

6. vaVOLUNTEER MODULE

This optional BTRS module enables administrators to manage contact lists, alerting and credentials management for volunteers and other special groups. Per feedback from the State of Michigan, Virtual Alert recognizes that we

should consider changing the name of this module. For the time being, this will remain the operating name for the module. The State of Michigan has indicated strong interest in this module and that it may desire to proceed forth quickly. Virtual Alert has segmented the various tasks and cost elements involved in designing, implementing and supporting this module. This is to enable the State of Michigan to determine which pieces can proceed forth immediately.

Business Rules Consulting

There is considerable work involved in guiding the State of Michigan through customization (to the degree allowed by the product) of processes, web site views and database structures for various groups. For such assistance, Virtual Alert will charge \$20,000 for the initial group to be established on this module. This work will commence with a multi-day onsite period with the working group that will establish such business rules. Thereafter, the bulk of assistance will take place remotely. This is the first task that can be undertaken to launch this module. We would expect that the State of Michigan can then take the bulk of responsibility for performing the business rules consulting for subsequent groups to be added. But Virtual Alert is willing to discuss support for subsequent groups at discounted rates.

Software License and Maintenance

The list price for vaVolunteer is a one-time license fee of \$75,000 per primary production database server. The spirit of the arrangement is that we will receive this one-time license for each separate production system that we have to install and support. The State of Michigan may establish back-up and test sites for no incremental license or software maintenance fees. If the State of Michigan purchases the software (defined as issuing a purchase order) before August 31, 2004, Virtual Alert is willing to sell the module to the State of Michigan for \$50,000.

THIS PRICING MAY NOT BE HONORED AFTER AUGUST 31, 2004 AND THE STATE OF MICHIGAN SHOULD EXPECT TO PAY LIST PRICE AFTER THAT DATE.

The maintenance rate for vaVolunteer will be 30% annually, paid up front and in full. As with the current BTRS standard software maintenance, this covers:

- Upgrades to subsequent versions of vaVolunteer for no incremental software fees
- Support for a up to five "super administrators". This does not include any support for "local" administrators or any end users

Installation

Installation for the State of Michigan will be \$10,000, to cover both a primary production site and a backup site. This pricing assumes that vaVolunteer will be installed within the same data centers as the rest of BTRS and added to the co-location arrangement. It also assumes a standard configuration, rather than any custom server/network configurations requested by the State of Michigan. This fee covers installation of the vaVolunteer software, hardware and 3rd party software, including networking aspects. This will also ensure that vaVolunteer successfully interacts with the rest of BTRS.

Co-location Fees

The list price for incremental servers added to the existing co-location arrangement (in same data centers as the rest of BTRS) is \$1000 per server per month. This may be subject to discounts (please see appropriate section). At this point in time, we are anticipating that vaVolunteer will require only one additional server per site. We reserve the right to change the recommended configuration for valid performance, functionality or security reasons that will be discussed with the State of Michigan, if they arise.

Configuration Fee

This fee covers the setup, in vaVolunteer, of an individual group. This is where the various processes (such as credentials management) are technically configured. It also includes structure of the database to ensure that the group can be successfully managed through the product. This configuration fee also includes setup of the website view for that particular group. The fee will be \$20,000 for each group that requires an individualized configuration of such processes, database structure and website view. Virtual Alert will require that a minimum of

one such configuration fee packages be purchased. Thereafter, the State of Michigan is free to perform subsequent configurations but will require technical training and is likely to require technical support from Virtual Alert to perform the first of such self-performed configurations.

Training

As with the rest of BTRS, training includes the provision of materials, as well as the execution of training. Training will continue at \$2000 per day. It is anticipated at this time that technical training will require 2 days and that administrative training will require 1 day. Given the numbers of end users involved, we do not anticipate that end users themselves would be trained, either by Virtual Alert or the State of Michigan. Rather, we recommend that the State of Michigan create some materials that can be sent to the various groups to explain the system, invite them to self-register, explain the registration process and anticipation of alert/notification drills.

Given all of the above, we anticipate that the State of Michigan will require 2 days of technical training and 2 days of administrative training, for a total of 4 training days costing \$8000 in fees.

Integration and Developer Support

All of the above items only cover a standard configuration install without integrating vaVolunteer with any other system than BTRS, as it currently stands at time of this letter. The State of Michigan has indicated that there may be great value in performing various levels of integrations of vaVolunteer with other Michigan applications (illustrative example: medical credentialing systems). Virtual Alert is qualified and very willing to perform multiple types of roles in such integrations. At one end of the spectrum, we are willing to be fully responsible for certain projects. At the other end of the spectrum, we can play a support-only role focused on how such integrations must interact with vaVolunteer. As explained in "Configuration Fee", this covers assistance for State of Michigan staff as they perform integration support for additional user groups. Our hourly rates will be \$145/hour for the project manager and \$120/hour for technicians. The State of Michigan should budget for at least 80 hours of assistance per group. We anticipate this would be higher than 80 hours for the first groups taken on by the State of Michigan, and lower for later groups, for various reasons.

All of the above items only cover a standard configuration install without integrating vaVolunteer with any other system than BTRS, as it currently stands at the time of this letter. The State of Michigan indicated that there may be great value in performing various levels of integrations of vaVolunteer with other Michigan applications (illustrative example: medical credentialing systems). Virtual Alert is qualified and very willing to perform multiple types of roles in such integrations. At one of the spectrum, we are willing to be fully responsible for certain projects. At the other end of the spectrum, we can play a support-only role focused on how such integrations must interact with vaVolunteer. At this time, it is very difficult to estimate the number of hours required for Virtual Alert staff. Upon request, Virtual Alert can provide a proposal to perform such work at the hourly rates presented above.

Third Party Components

We have included our estimates for the required hardware and software (assuming that the State of Michigan will continue with a primary site + backup site arrangement) in the attached spreadsheet. Our rough estimate is that the State of Michigan will need to invest in approximately \$38,000 of 3rd party components.

We would like to stress that this does not include a very important element – increased bandwidth for telephonic based alerting. Options for increasing bandwidth are presented within the spreadsheet section entitled "Potential 3rd Party Hardware/Software Upgrades for MIHAN – existing system". Virtual Alert is developing the capability to utilize standby providers to help execute "mass telephonic messaging". The State of Michigan may desire to increase its bandwidth through a combination of:

- Purchasing more owned infrastructure to add (more cards/T1's, potentially more servers depending upon how many cards would be added)
- Purchasing dedicated lines from a standby provider
- Purchasing surge capacity lines from a standby provider

EACH POTENTIAL COMBINATION HAS VERY DIFFERENT COST STRUCTURES AND PROS/CONS. THE STATE OF MICHIGAN WILL ALSO NEED TO DETERMINE HOW MUCH BANDWIDTH IT DESIRES, DEPENDING UPON HOW QUICKLY IT WANTS TELEPHONIC ALERTS TO BE EXECUTED, AND FOR WHICH AUDIENCES. ALSO, THE STATE OF MICHIGAN MAY WANT TO ALTER ITS

COMBINATION OVER TIME, AS THE POTENTIAL ALERTEE BASE GROWS OVER TIME. IT IS THEREFORE IMPOSSIBLE TO SET AN ESTIMATE ON THE COSTS INVOLVED. WE HAVE INCLUDED COSTING FOR A FEW OF THE OPTIONS IN THE ATTACHED SPREADSHEET. VIRTUAL ALERT ALSO CONTINUES TO PURSUE ADDITIONAL PARTNERSHIPS FOR STANDBY PROVIDERS, AS MORE COMPANIES CONTINUE TO GET INTO THIS BUSINESS OVER TIME – IT IS A YOUNG AND GROWING MARKET.

7. Geographic Information Systems Integration

This optional technical enhancement for BTRS starts with a requirements analysis. At completion of the requirements analysis and upon both parties achieving agreement regarding implementation, the State of Michigan may at its discretion initiate implementation.

Requirements Analysis

- **Summary Definition:** Virtual Alert would research the addition of map interfaces into the MIHAN core services. Research will produce technical assessment and recommendations, as well as costing for an actual implementation
- **Estimated Cost:** 24 hours of PM time; 80 hours of technician time. Total estimate for Virtual Alert professional fees = \$13,080

Implementation

- **Summary Definition:** Actual implementation of the solution recommended in the research option, agreed to by the State of Michigan and Virtual Alert, as scoped within that research project. The actual scope and costs cannot be known at this time
- **Estimated Implementation Cost:** 40 hours of PM time; 160 hours of technician time. Total estimate for Virtual Alert professional fees = \$25,000
- **Estimated Additional CoLo Fees:** Estimating addition of 4 servers (see below). List price for two sites = \$48,000 per year. Subject to discounts (see appropriate section)
 - **ESTIMATED 3RD PARTY COMPONENTS: APPROXIMATELY \$26,000. SEE ATTACHED SPREADSHEET**

8. Option 6: Additional BTRS User Licenses

The State of Michigan has expressed interest in the option of purchasing the following additional BTRS licenses:

**ADMINISTRATOR 100 @ \$495 LIST PRICE = \$49,500
EXTENDED LIST PRICE**

**COLLABORATOR 300 @ \$120 LIST PRICE = \$36,000
EXTENDED LIST PRICE**

<u>Alert-Only</u>	<u>1500 @ \$20 list price = \$30,000 extended list price</u>
Total	1900 = \$115,500 extended list price

Based on the prices established in our existing contract, definitions and prices for Alert-Only license types provided in Section 2 (these were not available at the time of the original contract), and that the State of Michigan currently owns 3,360 BTRS user licenses, per section I-VV of our current contract a 20% discount will apply to the first 140 licenses purchased and a 30% discount will apply to the next 1500, and a 35% discount will apply to the remaining 260 licenses purchased. Assuming the licenses are purchased as a single acquisition, Virtual Alert will apply the discount to the greatest advantage to the State of Michigan (i.e., the highest percentage discount will apply to the highest cost license) in the following manner.

Alert Only	140 x \$20 less 20% discount =	\$ 2,240
Alert Only	1360 x \$20 less 30% discount =	\$19,040
Collaborator	140 x \$120 less 30% discount =	\$11,760
Collaborator	160 x \$120 less 35% discount =	\$12,480
<u>Administrator</u>	<u>100 x \$495 less 35% discount =</u>	<u>\$32,175</u>
Total Price		\$77,695

This provides an average discount of 33% assuming all the licenses are acquired in one purchase.

Maintenance fees of 18% of list price annually as established in the maintenance agreement, pro-rated at a monthly rate through the end of the contract period will be due at purchase. Again assuming the licenses are acquired in a single purchase the additional annual maintenance will be \$20,790 (\$115,500 x 18%).

9. CO-LOCATION SERVICES

The table below details the unit pricing reflecting the cost of co-location services for managing a single system. The Site Setup Charge is a one-time fee. For the existing sites, the State of Michigan has already paid this fee and will not incur it again unless it requires Virtual Alert to set up the system in additional and/or different locations.

All other expenses are paid on a monthly basis. The table below indicates Virtual Alert's pricing for co-location services and the amounts due for renewing the current configuration through September 2004 assuming no modifications to the configuration. Fees will escalate by 3% for each contract year starting with October 1, 2004.

<i>One-time Expenses per Site</i>			
Item	Unit	Price	Extended Price
Site Setup Charge	0	\$3,000.00	\$0.00

<i>Current Monthly Recurring Expenses (Unit Pricing is per site)</i>			
Item	Unit	Price	Extended Price
Location Expense for pilot system	2	\$1,200.00	\$2,400.00
Internet Access, .5 - 2.5 Mbps Burstable, 95%*	2	\$750.00	\$1,500.00
Internet Access, 1.0 - 3.0 Mbps Burstable, 95%*	0	\$1,350.00	\$1,350.00
Internet Access, 2.0 - 10.0 Mbps Burstable, 95%*	0	\$2,700.00	\$2,700.00
System Services and Maintenance	2	\$2,100.00	\$4,200.00
Managed Security Devices	2	\$1,100.00	\$2,200.00
Administrative Review	2	\$1,700.00	\$3,400.00
Additional Server (Exchange Server)	2	\$1,000.00	\$2,000.00
Total Recurring Expenses per Site			\$15,700.00

Telephonic costs are not included because all telephonic charges (setup fees, fixed monthly expenses, variable costs) will be billed in full to the State of Michigan, at actual cost.

Services denoted by an asterisk "*" are invoiced based upon usage. Customer's Monthly Recurring Charge will vary depending on usage. The Monthly Recurring Charge set forth above for such usage based Service(s) is the minimum charge that may be assessed in any month.

Location Expense

The location expense provides for the secure facility in which the system will be housed. This facility provides the power needed to run the system, as well as an environment control system to maintain the optimal operating parameters for the system 24 hours a day, 7 days a week. Virtual Alert staff has 24x7 access to the location and can escalate to the co-location service provider.

Internet Access

Virtual Alert will provide for Internet connectivity in a metered fashion. The quotation above is for .5Mbps nominal that is burstable to 2.5Mbps. This means that during daily use the system will be running at .5Mbps but when an event drives use of the system up the system will accommodate for the added load by broadening the potential bandwidth to 2.5Mbps. This is billed at the 95th percentile. This means that there are frequent readings of the bandwidth that is being used and the client is billed at the average load over 95% of the time. With the number of users that the State of Michigan will initially put onto the system, we anticipate that it would be difficult for the State of Michigan to overload the .5Mbps that will be available. In the event that more bandwidth is needed, the State of Michigan will be billed commensurate with the load.

Virtual Alert will provide monthly usage analysis to the State of Michigan and review this with your system team. This will provide vital feedback to assess the success of the system, and will facilitate capacity planning.

System Services and Maintenance

Virtual Alert will monitor the applications that are used by the system to ensure that they are kept up to date and running properly. Virtual Alert will not add any updates or fixes without first verifying that they will not affect the system negatively, by testing the updates in Virtual Alert's test environment. This will be true for all of the applications that are loaded on the system, including the BTRS software.

Virtual Alert will backup the system once a day on an eight-week rotation. This will consist of full backups twice a week and incremental backups the other days. Once every rotation, Virtual Alert will run a full backup that will be stored in a remote location – away from where the system resides. This external backup can be used for Disaster Recovery or Operational Recovery purposes. Virtual Alert can ship tapes to the State of Michigan for a nominal extra fee.

Virtual Alert will monitor the entire system to ensure that it is constantly running at its peak performance. This will include providing reports and data to the State of Michigan about the system's performance and use. Further, Virtual Alert will monitor the overall health of the system and attempt to identify potential problems before they impact the day-to-day use of the system.

Manage Security Devices

Virtual Alert will ensure that the Cisco PIX, Microsoft Internet Security and Accelerator server and Cisco 3550 VLANs are kept up to date and monitored so that they will continuously provide the highest possible level of security for the State of Michigan's system. When combined with the Server Certificate to enable SSL-128 bit encrypted sessions, as per CDC Guidance, this provides transport level security to be available from the SSL Certificate provider. Virtual Alert understands that the information on the State of Michigan's HAN system is potentially sensitive and thus must be protected from unauthorized intrusion. Further, the proliferation of denial of service and other attacks on systems requires that the system be prepared to automatically fend off attacks that would prevent the use of the system. Virtual Alert will monitor the security systems and prevent these attacks from having an impact on the system.

Administrative Review

Virtual Alert will provide monthly reports organized in such a way that a non-technical person can understand. The reports will cover uptime, problems encountered, enhancements made, backups executed, usage levels and other information so that the State of Michigan will clearly understand the health and utilization of the system.

The complete reports will be posted to the system in a designated folder for easy review. Virtual Alert will also make itself available for conference calls, if so desired by the State of Michigan, to discuss the individual reports.

Installing Additional Servers

Virtual Alert will continue to add servers to the co-location centers at the rate of \$500 per server. These fees will not apply when an install fee has already been included for a new module such as vaVolunteer. We are willing to discuss discounts for large numbers of servers added at the same time. Virtual Alert will not charge for upgrading components of existing servers (i.e. add processors, add memory) as long as they can be performed during maintenance windows, according to a schedule set by Virtual Alert.

Discounted Co-location Services

Virtual Alert is willing to provide discounts off its standard rate of an incremental \$1000 per new server per month. These discounts will apply in general. The caveat that we must hold out is if incremental servers cause Virtual Alert to incur significant additional fees from its data center partners (i.e., add more racks, need more ISP drops). Virtual Alert will discuss these with the State of Michigan before final agreement is made on the incremental pricing for additional servers added to the co-location arrangement:

- For the next 5 servers added per site: no discount
- For the next 5 servers added per site: \$900 per server
- For the next 5 servers added per site: \$800 per server
- Beyond the 15th server added to each site: \$700 per server

STATE OF MICHIGAN
DEPARTMENT OF MANAGEMENT AND BUDGET
ACQUISITION SERVICES
P.O. BOX 30026, LANSING, MI 48909
OR
530 W. ALLEGAN, LANSING, MI 48933

September 25, 2003

CHANGE NOTICE NO. 2
TO
CONTRACT NO. 071B3001210
between
THE STATE OF MICHIGAN
and

NAME & ADDRESS OF VENDOR	TELEPHONE (512) 732-1214 Andrew Trickett
Virtual Alert Inc. P.O. Box 2985 LA Jolla, CA 92038 Andrew.trickett@virtualalert.com	VENDOR NUMBER/MAIL CODE
	BUYER (517) 373-7396 Andy Ghosh
Contract Administrator: Karen McMaster: (517) 335-8150 Health Alert Network (HAN) for Department of Community Health	
CONTRACT PERIOD: From: March 17, 2003 To: September 30, 2004	
TERMS N/A	SHIPMENT N/A
F.O.B. N/A	SHIPPED FROM N/A
MINIMUM DELIVERY REQUIREMENTS	
N/A	

NATURE OF CHANGE (S):

Effective immediately, this contract is EXTENDED through September 30, 2004.
The pricing terms and conditions remain the same.

AUTHORITY/REASON:

Per request from Sara Williams, DIT, dated 9/23/03.

TOTAL ESTIMATED CONTRACT VALUE REMAINS: \$1,216,935.70

STATE OF MICHIGAN
DEPARTMENT OF MANAGEMENT AND BUDGET
ACQUISITION SERVICES
P.O. BOX 30026, LANSING, MI 48909
OR
530 W. ALLEGAN, LANSING, MI 48933

March 24, 2003

CHANGE NOTICE NO. 1
TO
CONTRACT NO. 071B3001210
between
THE STATE OF MICHIGAN
and

NAME & ADDRESS OF VENDOR Virtual Alert Inc. P.O. Box 2985 LA Jolla, CA 92038	TELEPHONE (512) 732-1214 Andrew Trickett
	VENDOR NUMBER/MAIL CODE
	BUYER (517) 373-7396 Andy Ghosh
Contract Administrator: Karen McMaster: (517) 335-8150 Health Alert Network (HAN) for Department of Community Health	
CONTRACT PERIOD: From: March 17, 2003 To: September 30, 2003	
TERMS N/A	SHIPMENT N/A
F.O.B. N/A	SHIPPED FROM N/A
MINIMUM DELIVERY REQUIREMENTS	
N/A	

NATURE OF CHANGE (S):

1. The commodity code is changed to 918-29 (computer-software consultant) and the CS 138 number is 084S3000018.
2. The contract administrator for this contract is:

Sara Williams
Contract Mgmt. And Vendor Relations
Department of Information Technology
Phone: (517) 373-0984
Fax: (517) 241-7486
Email: Williamssa@michigan.gov

3. The project manager for this contract is:
Karen McMaster, Program Administrator
Office of Public Health Preparedness
Michigan Department of Community Health
3423 N. Martin Luther King Jr. Blvd.
Lansing, Michigan 48906
Phone: (517) 335-8150
Fax: (517) 335-9434
Email: MacMasterKaren@michigan.gov

071B3001210

All other terms and conditions remain the same.

AUTHORITY/REASON:

Per request from Sarah Williams, DIT, per email dated 3/19/03.

TOTAL ESTIMATED CONTRACT VALUE REMAINS: \$1,216,935.70

STATE OF MICHIGAN
DEPARTMENT OF MANAGEMENT AND BUDGET
ACQUISITION SERVICES
P.O. BOX 30026, LANSING, MI 48909
OR
530 W. ALLEGAN, LANSING, MI 48933

March 14, 2003

NOTICE
TO
CONTRACT NO. 071B3001210
between
THE STATE OF MICHIGAN
and

NAME & ADDRESS OF VENDOR	TELEPHONE (512) 732-1214 Andrew Trickett
Virtual Alert Inc. P.O. Box 2985 LA Jolla, CA 92038	VENDOR NUMBER/MAIL CODE
	BUYER (517) 373-7396 Andy Ghosh
Contract Administrator: Karen McMaster: (517) 335-8150 Health Alert Network (HAN) for Department of Community Health	
CONTRACT PERIOD: From: March 17, 2003 To: September 30, 2003	
TERMS N/A	SHIPMENT N/A
F.O.B. N/A	SHIPPED FROM N/A
MINIMUM DELIVERY REQUIREMENTS	
N/A	

The terms and conditions of this Contract are those of this Contract Agreement and the vendor's quote dated **January 10, 2003**. In the event of any conflicts between the specifications, terms and conditions indicated by the State and those indicated by the vendor, those of the State take precedence.

Estimated Contract Value: **\$1,216,935.70**

Date _____

**ACQUISITION SERVICES
STATE OF MICHIGAN
Health Alert Network (HAN) for DCH**

SECTION I – CONTRACTUAL SERVICES TERMS AND CONDITIONS

I-A	PURPOSE	1
I-B	TERM OF CONTRACT.....	1
I-C	ISSUING OFFICE	1
I-D	CONTRACT ADMINISTRATOR	1
I-E	PURCHASE ORDERS	2
I-F	COST LIABILITY	2
I-G	CONTRACTOR RESPONSIBILITIES.....	2
I-H	NEWS RELEASES	3
I-I	DISCLOSURE	3
I-J	ACCOUNTING RECORDS.....	3
I-K	INDEMNIFICATION.....	3
I-L	NON INFRINGEMENT/COMPLIANCE WITH LAWS	4
I-M	WARRANTIES AND REPRESENTATIONS.....	5
I-N	TIME IS OF THE ESSENCE	5
I-O	STAFFING OBLIGATIONS	5
I-P	CONFIDENTIALITY OF DATA AND INFORMATION.....	6
I-Q	REMEDIES FOR BREACH OF CONFIDENTIALITY	7
I-R	CONTRACTOR'S LIABILITY INSURANCE	7
I-S	NOTICE AND RIGHT TO CURE	9
I-T	CANCELLATION	9
I-U	RIGHTS AND OBLIGATIONS UPON CANCELLATION	10
I-V	EXCUSABLE FAILURE.....	11
I-W	ASSIGNMENT	12
I-X	DELEGATION.....	12
I-Y	NON-DISCRIMINATION CLAUSE	12
I-Z	WORKPLACE SAFETY AND DISCRIMINATORY HARASSMENT	12
I-AA	MODIFICATION OF SERVICE	12
I-BB	NOTICES.....	14
I-CC	ENTIRE AGREEMENT.....	14
I-DD	NO WAIVER OF DEFAULT.....	14
I-EE	SEVERABILITY	15
I-FF	HEADINGS.....	15
I-GG	RELATIONSHIP OF THE PARTIES	15
I-HH	UNFAIR LABOR PRACTICES	15
I-II	SURVIVOR.....	15
I-JJ	GOVERNING LAW	15
I-KK	YEAR 2000 SOFTWARE COMPLIANCE	15
I-LL	CONTRACT DISTRIBUTION.....	16
I-MM	STATEWIDE CONTRACTS.....	16
I-NN	STATE STANDARDS.....	16
I-OO	ELECTRONIC FUNDS TRANSFER	16
I-PP	TRANSITION ASSISTANCE.....	16

I-QQ DISCLOSURE OF LITIGATION.....	17
I-RR STOP WORK	18
I-SS PERFORMANCE AND RELIABILITY EVALUATION (PARE).....	19
I-TT SECURITY	21
I-UU SHIPPING AND SET UP COST ESTIMATE TO RELOCATE EQUIPMENTS TO MICHIGAN, UPON TERMINATION OF THE CONTRACT:	21
I-VV SECURITY	21

SECTION II - WORK STATEMENT

II-A TASKS.....	23
II-B OBJECTIVE.....	27
II-C PROJECT CONTROL AND REPORTS.....	28
II-D PRICE PROPOSAL.....	30

APPENDICES

- 1. Executive Summary**
- 2. Technical Proposal**
 - a. Virtual Alert Business Background**
 - b. Subcontracted Services – Equipment, Location, and Services**
 - c. Quotation Summary and Project Overview**
 - d. Hardware Listing**
 - e. Pricing Proposal for initial installation of BTRS**
 - f. Estimation template for 3rd party hardware and installation**
 - g. Configuration specification for MDCH**
- 3 Software License Agreement**
- 4 Equipment Location and Services Agreement**
- 5 Software Maintenance Agreement**
- 6 Three-party Escrow Agreement**

DEFINITION OF TERMS

TERMS	DEFINITIONS
Contract	Entire agreement means State of Michigan Contract, Software Source Code Escrow Agreement, Software License Agreement, Software Maintenance Agreement and Equipment Service Agreement
Contractor	Virtual Alert, Inc.
DMB	Michigan Department of Management and Budget
State	<p>The State of Michigan</p> <p>For Purposes of Indemnification as set forth in section I-J, State means the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees and agents.</p>
Blanket Purchase Order	Alternate term for “Contract” used in the State’s Computer system (Michigan Automated Information Network [MAIN])
Expiration	Except where specifically provided for in the Contract, the ending and termination of the contractual duties and obligations of the parties to the Contract pursuant to a mutually agreed upon date.
Cancellation	Ending all rights and obligations of the State and Contractor, except for any rights and obligations that are due and owing.



SECTION I CONTRACTUAL SERVICES TERMS AND CONDITIONS

I-A PURPOSE

This Contract is to obtain hardware, software, software maintenance, pre-installation consultation and training, and hosting services for the Michigan Health Alert Network for the Michigan Department of Community Health.

This Contract will be a Lump Sum/Fixed Price Contract.

I-B TERM OF CONTRACT

The State of Michigan is not liable for any cost incurred by the Contractor prior to signing of this Contract by all parties. The software, equipment and hosting services in this Contract cover the period March 17, 2003 through September 30, 2003. The State fiscal year is October 1st through September 30th. The Contractor should realize that payments in any given fiscal year are contingent upon enactment of legislative appropriations.

I-C ISSUING OFFICE

This Contract is issued by the State of Michigan, Department of Management and Budget (DMB), Acquisition Services, hereafter known as Acquisition Services, for the State of Michigan, Department of Community Health. Where actions are a combination of those of Acquisition Services and Department of Community Health, the authority will be known as the State.

Acquisition Services is the sole point of contact in the State with regard to all contractual matters relating to the services described herein. Acquisition Services is the only office authorized to change, modify, amend, alter, clarify, etc., the prices, specifications, terms, and conditions of this Contract. All communications concerning the prices, specifications, terms and conditions of this contract must be addressed to:

Andy Ghosh, Buyer Specialist
Technology and Professional Services Division
DMB, Acquisition Services
2nd Floor, Mason Building
P.O. Box 30026
Lansing, MI 48909
[Phone: \(517\) 373-7396](tel:5173737396)
[Email: ghosha@michigan.gov](mailto:ghosha@michigan.gov)

I-D CONTRACT ADMINISTRATOR

Upon receipt at Acquisition Services of the properly executed Contract Agreement, will administer this Contract on a day-to-day basis during the term of this Contract. However, administration of this Contract implies no authority to change, modify, clarify, amend, or otherwise alter the prices, terms, conditions, and specifications of this Contract. That authority is retained by Acquisition Services. The Contract Administrator for this project is:



Karen McMaster, Program Administrator
Office of Public Health Preparedness
Michigan Department of Community Health
3423 N. Martin Luther King, Jr. Blvd.
Lansing, Michigan 48906
Phone: 517-335-8150
Fax: 517-335-9434
Email MacMasterKaren@michigan .gov

I-E PURCHASE ORDERS

Orders for delivery of commodities and/or services may be issued directly by the State Departments through the issuance of a Purchase Order Form referencing this Contract (Blanket Purchase Order) agreement and the terms and conditions contained herein. Contractor is asked to reference the Purchase Order Number on all invoices for payment. The State of Michigan will provide a sales tax exemption certificate to the contractor. There will be no “vehicle costs” associated with this contract.

I-F COST LIABILITY

The State of Michigan assumes no responsibility or liability for costs incurred by the Contractor prior to the signing of this Contract. Total liability of the State is limited to the terms and conditions of this Contract.

I-G CONTRACTOR RESPONSIBILITIES

The Contractor is required to assume responsibility for all contractual activities offered in this Contract whether or not the Contractor performs them. Further, the State will consider the Prime Contractor to be the sole point of contact with regard to contractual matters, including but not limited to payment of any and all costs resulting from this Contract. If any part of the work is to be subcontracted, the contractor must notify the state and identify the subcontractor(s), including firm name and address, contact person, complete description of work to be subcontracted, and descriptive information concerning subcontractor's organizational abilities. The State reserves the right to approve subcontractors for this project and to require the Contractor to replace subcontractors found to be unacceptable. The Contractor is totally responsible for adherence by the subcontractor to all provisions of this Contract.

The authorized hosting subcontractors for this Contract are:

SureWest Communications
P.O. Box 969
Roseville, CA 95678
Richard P. Starr
916.746.3078

Inflow, Inc
8025 IH 35 North
Austin, TX 78753
Scott Rayer
512.531.5432



I-H NEWS RELEASES

News releases pertaining to this document or the services, study, data, or project to which it relates will not be made without prior written State approval, and then only in accordance with the explicit written instructions from the State. No results of the program are to be released without prior approval of the State and then only to persons designated.

I-I DISCLOSURE

All information in the Contractor's proposal and this Contract is subject to the provisions of the Freedom of Information Act, 1976 Public Act No. 442, as amended, MCL 15.231, *et seq.*.

I-J ACCOUNTING RECORDS

The Contractor is required to maintain all pertinent financial and accounting records and evidence pertaining to this Contract in accordance with generally accepted principles of accounting and other procedures specified by the State of Michigan. Financial and accounting records shall be made available, upon request, to the State of Michigan, its designees, or the Michigan Auditor General at any time during the Contract period and any extension thereof, and for three (3) years from the expiration date and final payment on this Contract or extension thereof.

I-K INDEMNIFICATION

A. General Indemnification

To the fullest extent permitted by law, the Contractor shall indemnify, defend and hold harmless the State, its departments, divisions, agencies, sections, commissions, officers, employees and agents, from and against all losses, liabilities, penalties, fines, damages and claims (including taxes), and all related costs and expenses (including reasonable attorneys' fees and disbursements and costs of investigation, litigation, settlement, judgments, interest and penalties), arising from or in connection with any of the following:

1. any claim, demand, action, citation or legal proceeding against the State, its employees and agents arising out of or resulting from (1) the product provided or (2) performance of the work, duties, responsibilities, actions or omissions of the Contractor or any of its subcontractors under this Contract.
2. any claim, demand, action, citation or legal proceeding against the State, its employees and agents arising out of or resulting from a breach by the Contractor of any representation or warranty made by the Contractor in this Contract;
3. any claim, demand, action, citation or legal proceeding against the State, its employees and agents arising out of or related to occurrences that the Contractor is required to insure against as provided for in this Contract;
4. any claim, demand, action, citation or legal proceeding against the State, its employees and agents arising out of or resulting from the death or bodily injury of any person, or the damage, loss or destruction of any real or tangible personal property, in connection with the performance of services by the Contractor, by any of its subcontractors, by anyone directly or indirectly employed by any of them, or by anyone for whose acts any of them may be liable; provided, however, that this indemnification obligation shall



not apply to the extent, if any, that such death, bodily injury or property damage is caused solely by the negligence or reckless or intentional wrongful conduct of the State;

5. any claim, demand, action, citation or legal proceeding against the State, its employees and agents which results from an act or omission of the Contractor or any of its subcontractors in its or their capacity as an employer of a person.

B. Patent/Copyright Infringement Indemnification

To the fullest extent permitted by law, the Contractor shall indemnify, defend and hold harmless the State, its employees and agents from and against all losses, liabilities, damages (including taxes), and all related costs and expenses (including reasonable attorneys' fees and disbursements and costs of investigation, litigation, settlement, judgments, interest and penalties) incurred in connection with any action or proceeding threatened or brought against the State to the extent that such action or proceeding is based on a claim that any piece of equipment, software, commodity or service supplied by the Contractor or its subcontractors, or the operation of such equipment, software, commodity or service, or the use or reproduction of any documentation provided with such equipment, software, commodity or service infringes any United States or foreign patent, copyright, trade secret or other proprietary right of any person or entity, which right is enforceable under the laws of the United States. In addition, should the equipment, software, commodity, or service, or the operation thereof, become or in the Contractor's opinion be likely to become the subject of a claim of infringement, the Contractor shall at the Contractor's sole expense (i) procure for the State the right to continue using the equipment, software, commodity or service or, if such option is not reasonably available to the Contractor, (ii) replace or modify the same with equipment, software, commodity or service of equivalent function and performance so that it becomes non-infringing, or, if such option is not reasonably available to Contractor, (iii) accept its return by the State with appropriate credits to the State against the Contractor's charges and reimburse the State for any losses or costs incurred as a consequence of the State ceasing its use and returning it.

C. Indemnification Obligation Not Limited

In any and all claims against the State of Michigan, or any of its agents or employees, by any employee of the Contractor or any of its subcontractors, the indemnification obligation under this Contract shall not be limited in any way by the amount or type of damages, compensation or benefits payable by or for the Contractor or any of its subcontractors under worker's disability compensation acts, disability benefits acts, or other employee benefits acts. This indemnification clause is intended to be comprehensive. Any overlap in subclauses, or the fact that greater specificity is provided as to some categories of risk, is not intended to limit the scope of indemnification under any other subclause.

D. Continuation of Indemnification Obligation

The duty to indemnify will continue in full force and affect notwithstanding the expiration or early termination of this Contract with respect to any claims based on facts or conditions, which occurred prior to termination.

I-L NON INFRINGEMENT/COMPLIANCE WITH LAWS

The Contractor warrants that in performing the services called for by this Contract it will not violate any applicable law, rule, or regulation, any contracts with third parties, or any intellectual



rights of any third party, including but not limited to, any United States patent, trademark, copyright, or trade secret.

I-M WARRANTIES AND REPRESENTATIONS

This Contract will contain customary representations and warranties by the Contractor, including, without limitation, the following:

1. The Contractor will perform all services in accordance with high professional standards in the industry;
2. The Contractor will use adequate numbers of qualified individuals with suitable training, education, experience and skill to perform the services;
3. The Contractor will use its best efforts to use efficiently any resources or services necessary to provide the services that are separately chargeable to the State;
4. The Contractor will use its best efforts to perform the services in the most cost effective manner consistent with the required level of quality and performance;
5. The Contractor will perform the services in a manner that does not infringe the proprietary rights of any third party;
6. The Contractor will perform the services in a manner that complies with all applicable laws and regulations;
7. The Contractor has duly authorized the execution, delivery and performance of this Contract;
8. The Contractor has not provided any gifts, payments or other inducements to any officer, employee or agent of the State;
9. The Contractor will maintain all equipment and software for which it has maintenance responsibilities in good operating condition and will undertake all repairs and preventive maintenance in accordance with applicable manufacturer's recommendations;
10. The Contractor will use its best efforts to ensure that no viruses or similar items are coded or introduced into the systems used to provide the services;
11. The Contractor will not insert or activate any disabling code into the systems used to provide the services without the State's prior written approval;
12. A ninety (90) day warranty on all purchased and developed software, data conversion programs, and data and customization to the product performed by the Contractor.

I-N TIME IS OF THE ESSENCE

The Contractor agrees that time is of the essence in the performance of the Contractor's obligations under this Contract.

I-O STAFFING OBLIGATIONS

The State reserves the right to approve the Contractor's assignment of Key Personnel to this project and to recommend reassignment of personnel deemed unsatisfactory by the State.



The Contractor shall not remove or reassign, without the State's prior written approval any of the Key Personnel until such time as the Key Personnel have completed all of their planned and assigned responsibilities in connection with performance of the Contractor's obligations under this Contract. The Contractor agrees that the continuity of Key Personnel is critical and agrees to the continuity of Key Personnel. Removal of Key Personnel without the written consent of the State may be considered by the State to be a material breach of this Contract. The prohibition against removal or reassignment shall not apply where Key Personnel must be replaced for reasons beyond the reasonable control of the Contractor including but not limited to illness, disability, resignation or termination of the Key Personnel's employment.

The State and the Contractor agree that the following personnel are Key Personnel for purposes of this Contract:

Name: Andrew Trickett Title: Chief Operating Officer

I-P CONFIDENTIALITY OF DATA AND INFORMATION

1. All financial, statistical, personnel, technical and other data and information relating to the State's operation which are designated confidential by the State and made available to the Contractor in order to carry out this Contract, or which become available to the Contractor in carrying out this Contract, shall be protected by the Contractor from unauthorized use and disclosure through the observance of the same or more effective procedural requirements as are applicable to the State. The identification of all such confidential data and information as well as the State's procedural requirements for protection of such data and information from unauthorized use and disclosure shall be provided by the State in writing to the Contractor. If the methods and procedures employed by the Contractor for the protection of the Contractor's data and information are deemed by the State to be adequate for the protection of the State's confidential information, such methods and procedures may be used, with the written consent of the State, to carry out the intent of this section.
2. The Contractor shall not be required under the provisions of this section to keep confidential, (1) information generally available to the public, (2) information released by the State generally, or to the Contractor without restriction, (3) information independently developed or acquired by the Contractor or its personnel without reliance in any way on otherwise protected information of the State. Notwithstanding the foregoing restrictions, the Contractor and its personnel may use and disclose any information which it is otherwise required by law to disclose, but in each case only after the State has been so notified, and has had the opportunity, if possible, to obtain reasonable protection for such information in connection with such disclosure.



I-Q REMEDIES FOR BREACH OF CONFIDENTIALITY

The Contractor acknowledges that a breach of its confidentiality obligations as set forth in section I-Q of this Contract shall be considered a material breach of this Contract. Furthermore the Contractor acknowledges that in the event of such a breach the State shall be irreparably harmed. Accordingly, if a court should find that the Contractor has breached or attempted to breach any such obligations, the Contractor will not oppose the entry of an appropriate order restraining it from any further breaches or attempted or threatened breaches. This remedy shall be in addition to and not in limitation of any other remedy or damages provided by law.

I-R CONTRACTOR'S LIABILITY INSURANCE

The Contractor is required to provide proof of the minimum levels of insurance coverage as indicated below. The purpose of this coverage shall be to protect the State from claims which may arise out of or result from the Contractor's performance of services under the terms of this Contract, whether such services are performed by the Contractor, or by any subcontractor, or by anyone directly or indirectly employed by any of them, or by anyone for whose acts they may be liable.

The Contractor waives all rights against the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees and agents for recovery of damages to the extent these damages are covered by the insurance policies the Contractor is required to maintain pursuant to this Contract. The Contractor also agrees to provide evidence that all applicable insurance policies contain a waiver of subrogation by the insurance company.

All insurance coverages provided relative to this Contract/Purchase Order is PRIMARY and NON-CONTRIBUTING to any comparable liability insurance (including self-insurances) carried by the State.

The Insurance shall be written for not less than any minimum coverage herein specified or required by law, whichever is greater. All deductible amounts for any of the required policies are subject to approval by the State.

The State reserves the right to reject insurance written by an insurer the State deems unacceptable.

BEFORE THE CONTRACT IS SIGNED BY BOTH PARTIES OR BEFORE THE PURCHASE ORDER IS ISSUED BY THE STATE, THE CONTRACTOR MUST FURNISH TO THE DIRECTOR OF ACQUISITION SERVICES, CERTIFICATE(S) OF INSURANCE VERIFYING INSURANCE COVERAGE. THE CERTIFICATE MUST BE ON THE STANDARD "ACCORD" FORM. THE CONTRACT OR PURCHASE ORDER NO. MUST BE SHOWN ON THE CERTIFICATE OF INSURANCE TO ASSURE CORRECT FILING. All such Certificate(s) are to be prepared and submitted by the Insurance Provider and not by the Contractor. All such Certificate(s) shall contain a provision indicating that coverages afforded under the policies WILL NOT BE CANCELLED, MATERIALLY CHANGED, OR NOT RENEWED without THIRTY (30) days prior written notice, except for 10 days for non-payment of premium, having been given to the Director of Acquisition Services, Department of Management and Budget. Such NOTICE must include the CONTRACT NUMBER affected and be mailed to: Director, Acquisition Services, Department of Management and Budget, P.O. Box 30026, Lansing, Michigan 48909.



The Contractor is required to provide the type and amount of insurance checked (☑) below:

- ☑ 1. Commercial General Liability with the following minimum coverages:

\$2,000,000 General Aggregate Limit other than Products/Completed Operations
 \$2,000,000 Products/Completed Operations Aggregate Limit
 \$1,000,000 Personal & Advertising Injury Limit
 \$1,000,000 Each Occurrence Limit
 \$500,000 Fire Damage Limit (any one fire)

The Contractor must list the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees and agents as ADDITIONAL INSURED on the Commercial General Liability policy.

- ☑ 2. If a motor vehicle is used to provide services or products under this Contract, the Contractor must have vehicle liability insurance on any auto including owned, hired and non-owned vehicles used in Contractor's business for bodily injury and property damage as required by law.

The Contractor must list the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees and agents as ADDITIONAL INSURED on the vehicle liability policy.

- ☑ 3. Worker's disability compensation, disability benefit or other similar employee benefit act with minimum statutory limits. NOTE: (1) If coverage is provided by a State fund or if Contractor has qualified as a self-insurer, separate certification must be furnished that coverage is in the state fund or that Contractor has approval to be a self-insurer; (2) Any citing of a policy of insurance must include a listing of the States where that policy's coverage is applicable; and (3) Any policy of insurance must contain a provision or endorsement providing that the insurers' rights of subrogation are waived. This provision shall not be applicable where prohibited or limited by the laws of the jurisdiction in which the work is to be performed.

- ☐ 4. For contracts providing temporary staff personnel to the State, the Contractor shall provide an Alternate Employer Endorsement with minimum coverage of \$1,000,000.

- ☑ 5. Employers liability insurance with the following minimum limits:

\$100,000 each accident
 \$100,000 each employee by disease
 \$500,000 aggregate disease

- ☑ 6. Claims for damages because of injury to or destruction of tangible property, including loss of use resulting therefrom, subject to a limit of liability of not less than \$50,000.00 each occurrence for non-automobile hazards and as required by law for automobile hazards.



I-S NOTICE AND RIGHT TO CURE

In the event of a curable breach by the Contractor, the State shall provide the Contractor written notice of the breach and a time period to cure said breach described in the notice. This section requiring notice and an opportunity to cure shall not be applicable in the event of successive or repeated breaches of the same nature or if the State determines in its sole discretion that the breach poses a serious and imminent threat to the health or safety of any person or the imminent loss, damage or destruction of any real or tangible personal property.

I-T CANCELLATION

The State may cancel this Contract without further liability or penalty to the State, its departments, divisions, agencies, offices, commissions, officers, agents and employees for any of the following reasons:

1. Material Breach by the Contractor. In the event that the Contractor breaches any of its material duties or obligations under this Contract, which are either not capable of or subject to being cured, or are not cured within the time period specified in the written notice of breach provided by the State, or pose a serious and imminent threat to the health and safety of any person, or the imminent loss, damage or destruction of any real or tangible personal property, the State may, having provided written notice of cancellation to the Contractor, cancel this Contract in whole or in part, for cause, as of the date specified in the notice of cancellation.

In the event that this Contract is cancelled for cause, in addition to any legal remedies otherwise available to the State by law or equity, the Contractor shall be responsible for all costs incurred by the State in canceling this Contract, including but not limited to, State administrative costs, attorneys fees and court costs, and any additional costs the State may incur to procure the services required by this Contract from other sources. All excess procurement costs and damages shall not be considered by the parties to be consequential, indirect or incidental, and shall not be excluded by any other terms otherwise included in this Contract.

In the event the State chooses to partially cancel this Contract for cause charges payable under this Contract will be equitably adjusted to reflect those services that are cancelled.

In the event this Contract is cancelled for cause pursuant to this section, and it is therefore determined, for any reason, that the Contractor was not in breach of contract pursuant to the provisions of this section, that cancellation for cause shall be deemed to have been a cancellation for convenience, effective as of the same date, and the rights and obligations of the parties shall be limited to that otherwise provided in this Contract for a cancellation for convenience.

2. Cancellation For Convenience By the State. The State may cancel this Contract for its convenience, in whole or part, if the State determines that such a cancellation is in the State's best interest. Reasons for such cancellation shall be left to the sole discretion of the State and may include, but not necessarily be limited to (a) the State no longer needs the services or products specified in this Contract, (b) relocation of office, program changes, changes in laws, rules, or regulations make implementation of this Contract services no longer practical or feasible, and (c) unacceptable prices for additional services requested by the State. The



State may cancel the Contract for its convenience, in whole or in part, by giving the Contractor written notice 30 days prior to the date of cancellation. If the State chooses to cancel this Contract in part, the charges payable under this Contract shall be equitably adjusted to reflect those services that are cancelled.

3. Non-Appropriation. In the event that funds to enable the State to effect continued payment under this Contract are not appropriated or otherwise made available. The Contractor acknowledges that, if this Contract extends for several fiscal years, continuation of this Contract is subject to appropriation or availability of funds for this project. If funds are not appropriated or otherwise made available, the State shall have the right to cancel this Contract at the end of the last period for which funds have been appropriated or otherwise made available by giving written notice of cancellation to the Contractor. The State shall give the Contractor written notice of such non-appropriation or unavailability within 30 days after it receives notice of such non-appropriation or unavailability.
4. Criminal Conviction. In the event the Contractor, an officer of the Contractor, or an owner of a 25% or greater share of the Contractor, is convicted of a criminal offense incident to the application for or performance of a State, public or private Contract or subcontract; or convicted of a criminal offense including but not limited to any of the following: embezzlement, theft, forgery, bribery, falsification or destruction of records, receiving stolen property, attempting to influence a public employee to breach the ethical conduct standards for State of Michigan employees; convicted under State or federal antitrust statutes; or convicted of any other criminal offense which in the sole discretion of the State, reflects upon the Contractor's business integrity.
5. Approvals Rescinded. In the event any final administrative or judicial decision or adjudication disapproves a previously approved request for purchase of personal services pursuant to Article 11, Section 5 of the Michigan Constitution of 1963, and Chapter 7 of the Civil Service Rules. Notwithstanding any other provision of this Contract to the contrary, the State Personnel Director is authorized to disapprove contractual disbursements for personal services if the Director determines that this Contract of the disbursements under this Contract violate Article 11, Section 5 of the Constitution or violate applicable Civil Service rules or regulations. Cancellation may be in whole or in part and may be immediate as of the date of the written notice to the Contractor or may be effective as of the date stated in such written notice.

I-U RIGHTS AND OBLIGATIONS UPON CANCELLATION

1. If this Contract is canceled by the State for any reason, the Contractor shall, (a) stop all work as specified in the notice of cancellation, (b) take any action that may be necessary, or that the State may direct, for preservation and protection of Work Product or other property derived or resulting from this Contract that may be in the Contractor's possession, (c) return all materials and property provided directly or indirectly to the Contractor by any entity, agent or employee of the State, (d) transfer title and deliver to the State, unless otherwise directed by this Contract Administrator or his or her designee, all Work Product resulting from this Contract, and (e) take any action to mitigate and limit any potential damages, or requests for Contractor adjustment or cancellation settlement costs, to the maximum practical extent, including, but not limited to, canceling or limiting as otherwise applicable, those subcontracts, and outstanding orders for material and supplies resulting from the canceled Contract.
2. In the event the State cancels this Contract prior to its expiration for its own convenience, the State shall pay the Contractor for all charges due for services provided prior to the date of



cancellation and if applicable as a separate item of payment pursuant to this Contract, for partially completed Work Product, on a percentage of completion basis. In the event of a cancellation for cause, or any other reason under this Contract, the State will pay, if applicable, as a separate item of payment pursuant to this Contract, for all partially completed Work Products, to the extent that the State requires the Contractor to submit to the State any such deliverables, and for all charges due under this Contract for any cancelled services provided by the Contractor prior to the cancellation date. All completed or partially completed Work Product prepared by the Contractor pursuant to this Contract shall, at the option of the State, become the State's property, and the Contractor shall be entitled to receive just and fair compensation for such Work Product. Regardless of the basis for the cancellation, the State shall not be obligated to pay, or otherwise compensate, the Contractor for any lost expected future profits, costs or expenses incurred with respect to Services not actually performed for the State.

3. If any such cancellation by the State is for cause, the State shall have the right to set-off against any amounts due the Contractor, the amount of any damages for which the Contractor is liable to the State under this Contract or pursuant to law and equity.
4. Upon a good faith cancellation, the State shall have the right to assume, at its option, any and all subcontracts and agreements for services and materials provided under this Contract, and may further pursue completion of the Work Product under this Contract by replacement contract or otherwise as the State may in its sole judgment deem expedient.

I-V EXCUSABLE FAILURE

1. Neither party shall be liable for any default or delay in the performance of its obligations under this Contract if and to the extent such default or delay is caused, directly or indirectly, by: fire, flood, earthquake, elements of nature or acts of God; riots, civil disorders, rebellions or revolutions in any country; the failure of the other party to perform its material responsibilities under this Contract (either itself or through another contractor); injunctions (provided the injunction was not issued as a result of any fault or negligence of the party seeking to have its default or delay excused); or any other cause beyond the reasonable control of such party; provided the non-performing party and its subcontractors are without fault in causing such default or delay, and such default or delay could not have been prevented by reasonable precautions and cannot reasonably be circumvented by the non-performing party through the use of alternate sources, workaround plans or other means, including disaster recovery plans. In such event, the non-performing party will be excused from any further performance or observance of the obligation(s) so affected for as long as such circumstances prevail and such party continues to use its best efforts to recommence performance or observance whenever and to whatever extent possible without delay provided such party promptly notifies the other party in writing of the inception of the excusable failure occurrence, and also of its abatement or cessation.
2. If any of the above enumerated circumstances substantially prevent, hinder, or delay performance of the services necessary for the performance of the State's functions for more than 14 consecutive days, and the State determines that performance is not likely to be resumed within a period of time that is satisfactory to the State in its reasonable discretion, then at the State's option: (a) the State may procure the affected services from an alternate source, and the State shall not be liable for payments for the unperformed services under this Contract for so long as the delay in performance shall continue; (b) the State may cancel any portions of this Contract so affected and the charges payable thereunder shall be equitably adjusted to reflect those services canceled; or (c) this Contract will be canceled without liability of the State to the Contractor as of the date specified by the State in a written notice



of cancellation to the Contractor. The Contractor will not have the right to any additional payments from the State as a result of any excusable failure occurrence or to payments for services not rendered as a result of the excusable failure condition. Defaults or delays in performance by the Contractor which are caused by acts or omissions of its subcontractors will not relieve the Contractor of its obligations under this Contract except to the extent that a subcontractor is itself subject to any excusable failure condition described above and the Contractor cannot reasonably circumvent the effect of the subcontractor's default or delay in performance through the use of alternate sources, workaround plans or other means.

I-W ASSIGNMENT

The Contractor shall not have the right to assign this Contract or to assign or delegate any of its duties or obligations under this Contract to any other party (whether by operation of law or otherwise), without the prior written consent of the State. Any purported assignment in violation of this section shall be null and void. Further, the Contractor may not assign the right to receive money due under this Contract without the prior written consent of the Director of Acquisition Services.

I-X DELEGATION

The Contractor shall not delegate any duties or obligations under this Contract to a subcontractor other than a subcontractor named in the bid unless the Director of Acquisition Services has given written consent to the delegation.

I-Y NON-DISCRIMINATION CLAUSE

In the performance of this Contract, the Contractor agrees not to discriminate against any employee or applicant for employment, with respect to their hire, tenure, terms, conditions or privileges of employment, or any matter directly or indirectly related to employment, because of race, color, religion, national origin, ancestry, age, sex, height, weight, marital status, physical or mental disability unrelated to the individual's ability to perform the duties of the particular job or position. The Contractor further agrees that every subcontract entered into for the performance of this Contract will contain a provision requiring non-discrimination in employment, as herein specified, binding upon each subcontractor. This covenant is required pursuant to the Elliot Larsen Civil Rights Act, 1976 Public Act 453, as amended, MCL 37.2101, *et seq*, and the Persons with Disabilities Civil Rights Act, 1976 Public Act 220, as amended, MCL 37.1101, *et seq*, and any breach thereof may be regarded as a material breach of this Contract.

I-Z WORKPLACE SAFETY AND DISCRIMINATORY HARASSMENT

In performing services for the State pursuant to this Contract, the Contractor shall comply with Department of Civil Service Rules 2-20 regarding Workplace Safety and 1-8.3 regarding Discriminatory Harassment. In addition, the Contractor shall comply with Civil Service Regulations governing workplace safety and discriminatory harassment and any applicable state agency rules on these matters that the agency provides to the Contractor. Department of Civil Service Rules and Regulations can be found on the Department of Civil Service website at www.state.mi.us/mdcs/Regindx.

I-AA MODIFICATION OF SERVICE



The Director of Acquisition Services reserves the right to modify this service during the course of this Contract. Such modification may include adding or deleting tasks that this service shall encompass and/or any other modifications deemed necessary.

This Contract may not be revised, modified, amended, extended, or augmented, except by a writing executed by the parties hereto, and any breach or default by a party shall not be waived or released other than in writing signed by the other party.

The State reserves the right to request from time to time, any changes to the requirements and specifications of this Contract and the work to be performed by the Contractor under this Contract. The Contractor shall provide a change order process and all requisite forms. The State reserves the right to negotiate the process during contract negotiation. At a minimum, the State would like the Contractor to provide a detailed outline of all work to be done, including tasks necessary to accomplish the deliverables, timeframes, listing of key personnel assigned, estimated hours for each individual per task, and a complete and detailed cost justification.

1. Within five (5) business days of receipt of a request by the State for any such change, or such other period of time as to which the parties may agree mutually in writing, the Contractor shall submit to the State a proposal describing any changes in products, services, timing of delivery, assignment of personnel, and the like, and any associated price adjustment. The price adjustment shall be based on a good faith determination and calculation by the Contractor of the additional cost to the Contractor in implementing the change request less any savings realized by the Contractor as a result of implementing the change request. The Contractor's proposal shall describe in reasonable detail the basis for the Contractor's proposed price adjustment, including the estimated number of hours by task by labor category required to implement the change request.
2. If the State accepts the Contractor's proposal, it will issue a change notice and the Contractor will implement the change request described therein. The Contractor will not implement any change request until a change notice has been issued validly. The Contractor shall not be entitled to any compensation for implementing any change request or change notice except as provided explicitly in an approved change notice.
3. If the State does not accept the Contractor's proposal, the State may:
 - a. withdraw its change request; or
 - b. modify its change request, in which case the procedures set forth above will apply to the modified change request.

If the State requests or directs the Contractor to perform any activities that are outside the scope of the Contractor's responsibilities under this Contract ("New Work"), the Contractor must notify the State promptly, and before commencing performance of the requested activities, that it believes the requested activities are New Work. If the Contractor fails to so notify the State prior to commencing performance of the requested activities, any such activities performed before notice is given by the Contractor shall be conclusively considered to be In-scope Services, not New Work.

If the State requests or directs the Contractor to perform any services or functions that are consistent with and similar to the services being provided by the Contractor under this Contract, but which the Contractor reasonably and in good faith believes are not included within the scope of the Contractor's responsibilities and charges as set forth in this Contract, then prior to performing such services or function, the Contractor shall promptly notify the State in writing that it considers the services or function to be an "Additional Service" for which the Contractor should receive additional compensation. If the Contractor does not so notify the State, the



Contractor shall have no right to claim thereafter that it is entitled to additional compensation for performing such services or functions. If the Contractor does so notify the State, then such a service or function shall be governed by the change request procedure set forth in the preceding paragraph.

IN THE EVENT PRICES ARE NOT ACCEPTABLE TO THE STATE, THE CONTRACT SHALL BE SUBJECT TO COMPETITIVE BIDDING BASED UPON THE NEW SPECIFICATIONS.

I-BB NOTICES

Any notice given to a party under this Contract must be written and shall be deemed effective, if addressed to such party as addressed below upon (i) delivery, if hand delivered; (ii) receipt of a confirmed transmission by facsimile if a copy of the notice is sent by another means specified in this section; (iii) the third (3rd) Business Day after being sent by U.S. mail, postage pre-paid, return receipt requested; or (iv) the next Business Day after being sent by a nationally recognized overnight express courier with a reliable tracking system.

For the Contractor: Andrew Trickett
 7000 Bee Cave Road, Suite 300
 Austin, Texas 78746
 Phone: 512-732-1214.

For the State: Andy Ghosh, Buyer Specialist
 DMB, Acquisition Services
 Tactical Purchasing
 2nd Floor, Mason Building
 P.O. Box 30026
 Lansing, MI 48909

Either party may change its address where notices are to be sent giving written notice in accordance with this section.

I-CC ENTIRE AGREEMENT

This Contract represents the entire agreement between the parties and supersedes all proposals or other prior agreements, oral or written, and all other communications between the parties relating to this subject.

I-DD NO WAIVER OF DEFAULT

The failure of a party to insist upon strict adherence to any term of this Contract shall not be considered a waiver or deprive the party of the right thereafter to insist upon strict adherence to that term, or any other term, of this Contract.



I-EE SEVERABILITY

Each provision of this Contract shall be deemed to be severable from all other provisions of this Contract and, if one or more of the provisions of this Contract shall be declared invalid, the remaining provisions of this Contract shall remain in full force and effect.

I-FF HEADINGS

Captions and headings used in this Contract are for information and organization purposes. Captions and headings, including inaccurate references, do not, in any way, define or limit the requirements or terms and conditions of this Contract.

I-GG RELATIONSHIP OF THE PARTIES

The relationship between the State and the Contractor is that of client and independent Contractor. No agent, employee, or servant of the Contractor or any of its subcontractors shall be or shall be deemed to be an employee, agent, or servant of the State for any reason. The Contractor will be solely and entirely responsible for its acts and the acts of its agents, employees, servants and subcontractors during the performance of this Contract.

I-HH UNFAIR LABOR PRACTICES

Pursuant to 1980 Public Act 278, as amended, MCL 423.231, et seq, the State shall not award a Contract or subcontract to an employer whose name appears in the current register of employers failing to correct an unfair labor practice compiled pursuant to section 2 of the Act. This information is compiled by the United States National Labor Relations Board.

A Contractor of the State, in relation to this Contract, shall not enter into a Contract with a subcontractor, manufacturer, or supplier whose name appears in this register. Pursuant to section 4 of 1980 Public Act 278, MCL 423.324, the State may void this Contract if, subsequent to award of this Contract, the name of the Contractor as an employer, or the name of the subcontractor, manufacturer or supplier of the Contractor appears in the register.

I-II SURVIVOR

Any provisions of this Contract that impose continuing obligations on the parties including, but not limited to the Contractor's indemnity and other obligations shall survive the expiration or cancellation of this Contract for any reason.

I-JJ GOVERNING LAW

This Contract shall in all respects be governed by, and construed in accordance with, the laws of the State of Michigan. Any dispute arising herein shall be resolved in the State of Michigan.

I-KK YEAR 2000 SOFTWARE COMPLIANCE

The Contractor warrants that all software for which the Contractor either sells or licenses to the State of Michigan and used by the State prior to, during or after the calendar year 2000, includes or shall include, at no added cost to the State, design and performance so the State shall not experience software abnormality and/or the generation of incorrect results from the software, due to date oriented processing, in the operation of the business of the State of Michigan.



The software design, to insure year 2000 compatibility, shall include, but is not limited to: data structures (databases, data files, etc.) that provide 4-digit date century; stored data that contain date century recognition, including, but not limited to, data stored in databases and hardware device internal system dates; calculations and program logic (e.g., sort algorithms, calendar generation, event recognition, and all processing actions that use or produce date values) that accommodates same century and multi-century formulas and date values; interfaces that supply data to and receive data from other systems or organizations that prevent non-compliant dates and data from entering any State system; user interfaces (i.e., screens, reports, etc.) that accurately show 4 digit years; and assurance that the year 2000 shall be correctly treated as a leap year within all calculation and calendar logic.

I-LL CONTRACT DISTRIBUTION

Acquisition Services shall retain the sole right of Contract distribution to all State agencies and local units of government unless other arrangements are authorized by Acquisition Services.

I-MM STATEWIDE CONTRACTS

If this Contract is for the use of more than one agency and if the goods or services provided under this Contract do not meet the form, function and utility required by an agency, that agency may, subject to state purchasing policies, procure the goods or services from another source.

I-NN STATE STANDARDS

PM METHODOLOGY STANDARDS. The State has adopted a standard, documented Project Management Methodology (PMM) for use on all Information Technology (IT) based projects. This policy is referenced in the document titled "Project Management Methodology" – DMB Administrative Guide Procedure 1380.02 issued June 2000. Vendors may obtain a copy of this procedure by contacting the DMB Office of Information Technology Solutions.

The Contractor shall use the State's PMM to manage State of Michigan Information Technology (IT) based projects. The requesting agency will provide the applicable documentation and internal agency processes for the methodology. If the Contractor requires training on the methodology, those costs shall be the responsibility of the Contractor, unless otherwise stated.

Contractor will provide data to prepare progress reports. Schedules, deliverables, and planning are completed and part of contract already. MDCH will monitor progress and ensure compliance with PMM and bear primary responsibility for project management.

I-OO ELECTRONIC FUNDS TRANSFER

Electronic transfer of funds is available to State Contractors. Contractors are encouraged to register with the State of Michigan Office of Financial Management so the State can make payments related to this Contract electronically at www.cpexpress.state.mi.us.

I-PP TRANSITION ASSISTANCE

If this Contract is not renewed at the end of this term, or is canceled prior to its expiration, for any reason, the Contractor must provide for up to Six (6) Months after the expiration or cancellation of this Contract, all reasonable transition assistance requested by the State, to allow for the expired or canceled portion of the Services to continue without interruption or adverse effect, and to facilitate the orderly transfer of such services to the State or its designees. Such transition



assistance will be deemed by the parties to be governed by the terms and conditions of this Contract, (notwithstanding this expiration or cancellation) except for those Contract terms or conditions that do not reasonably apply to such transition assistance. The State shall pay the Contractor for any resources utilized in performing such transition assistance at the most current rates provided by the Contract for Contractor performance. If the State cancels this Contract for cause, then the State will be entitled to off set the cost of paying the Contractor for the additional resources the Contractor utilized in providing transition assistance with any damages the State may have otherwise accrued as a result of said cancellation.

I-QQ DISCLOSURE OF LITIGATION

1. The Contractor shall notify the State, if it, or any of its subcontractors, or their officers, directors, or key personnel under this Contract, have ever been convicted of a felony, or any crime involving moral turpitude, including, but not limited to fraud, misappropriation or deception. Contractor shall promptly notify the State of any criminal litigation, investigations or proceeding which may have arisen or may arise involving the Contractor or any of the Contractor's subcontractor, or any of the foregoing entities' then current officers or directors during the term of this Contract and three years thereafter.
2. The Contractor shall notify the State promptly of any civil litigation, arbitration, proceeding, or judgments that may have arisen against it or its subcontractors during the five years proceeding the contract date or which may occur during the term of this Contract or three years thereafter, which involve (1) products or services similar to those provided to the State under this Contract and which either involve a claim in excess of \$250,000 or which otherwise may affect the viability or financial stability of the Contractor , or (2) a claim or written allegation of fraud by the Contractor or any subcontractor hereunder, arising out of their business activities, or (3) a claim or written allegation that the Contractor or any subcontractor hereunder violated any federal, state or local statute, regulation or ordinance. Multiple lawsuits and or judgments against the Contractor or subcontractor, in any an amount less than \$250,000 shall be disclosed to the State to the extent they affect the financial solvency and integrity of the Contractor or subcontractor.
3. All notices under subsection 1 and 2 herein shall be provided in writing to the State within fifteen business days after the Contractor learns about any such criminal or civil investigations and within fifteen days after the commencement of any proceeding, litigation, or arbitration, as otherwise applicable. Details of settlements, which are prevented from disclosure by the terms of the settlement, shall be annotated as such. Semi-annually, during the term of this Contract, and thereafter for three years, Contractor shall certify that it is in compliance with this Section. Contractor may rely on similar good faith certifications of its subcontractors, which certifications shall be available for inspection at the option of the State.
4. Assurances - In the event that such investigation, litigation, arbitration or other proceedings disclosed to the State pursuant to this Section, or of which the State otherwise becomes aware, during the term of this Contract, causes the State to be reasonably concerned about:
 - a. the ability of the Contractor or its subcontractor to continue to perform this Contract in accordance with its terms and conditions, or
 - b. whether the Contractor or its subcontractor in performing services is engaged in conduct which is similar in nature to conduct alleged in such investigation, litigation, arbitration or other proceedings, which conduct would constitute a breach of this Contract or violation of Michigan or Federal law, regulation or public policy, then



The Contractor shall be required to provide the State all reasonable assurances requested by the State to demonstrate that: (a) the Contractor or its subcontractors hereunder will be able to continue to perform this Contract in accordance with its terms and conditions, (b) the Contractor or its subcontractors will not engage in conduct in performing services under this Contract which is similar in nature to the conduct alleged in any such litigation, arbitration or other proceedings.

5. The Contractor's failure to fully and timely comply with the terms of this section, including providing reasonable assurances satisfactory to the State, may constitute a material breach of this Contract.

I-RR STOP WORK

1. The State may, at any time, by written stop work order to the Contractor, require that the Contractor stop all, or any part, of the work called for by this Contract for a period of up to 90 days after the stop work order is delivered to the Contractor, and for any further period to which the parties may agree. The stop work order shall be specifically identified as such and shall indicate that it is issued under this section. Upon receipt of the stop work order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the stop work order during the period of work stoppage. Within the period of the stop work order, the State shall either:
 - a. Cancel the stop work order; or
 - b. Cancel the work covered by the stop work order as provided in the cancellation section of this Contract.
2. If a stop work order issued under this section is canceled or the period of the stop work order or any extension thereof expires, the Contractor shall resume work. The State shall make an equitable adjustment in the delivery schedule, the contract price, or both, and the Contract shall be modified, in writing, accordingly, if:
 - a. The stop work order results in an increase in the time required for, or in the Contractor's costs properly allocable to the performance of any part of this Contract; and
 - b. The Contractor asserts its right to an equitable adjustment within 30 days after the end of the period of work stoppage; provided, that if the State decides the facts justify the action, the State may receive and act upon a proposal submitted at any time before final payment under this Contract.
3. If the stop work order is not canceled and the work covered by the stop work order is canceled for reasons other than material breach, the State shall allow reasonable costs resulting from the stop work order in arriving at the cancellation settlement.
4. If a stop work order is not canceled and the work covered by the stop work order is canceled for material breach, the State shall not allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop work order.



5. An appropriate equitable adjustment may be made in any related contract of the Contractor that provides for adjustment and is affected by any stop work order under this section. The State shall not be liable to the Contractor for loss of profits because of a stop work order issued under this section.

I-SS PERFORMANCE AND RELIABILITY EVALUATION (PARE)

The State requires that a performance and reliability evaluation (PARE) is to be performed for this Contract. The State of Michigan will pay for co-location fees during the PARE process. The standard of performance for the PARE will be closely monitored during the acceptance period.

The Performance and Reliability Evaluation will consist of two phases.

1. PHASE I

The first phase shall be comprised of a specification compliance review of the equipment listed on the ordering documents. Such equipment shall be checked for total compliance with all required specifications of this Contract. In the event that the State determines that any component or feature of the delivered equipment or software does not comply with the mandatory specifications of this Contract, the State shall so notify the Contractor, allowing 14 calendar days for rectification by the Contractor. Should the Contractor be unable to rectify the deficiency, the State reserves the right to cancel the ordering document. Should the equipment and software pass the specification conformance review, the equipment shall enter Phase II of the PARE.

Phase I will be deemed accepted when the contractor provides a copy of official documentation from Dell describing the delivered systems with a letter attesting to receipt and verification of the hardware specified in Appendix 2 (d).

2. PHASE II

Basic loads will be used for testing Customization, which is not anticipated at this time, can come after PARE. Contractor must make a backup of the system after initial installation and inform MDCH when back up is complete prior to initiating testing and therefore to minimize rebuild effort. Contractor will instruct MDCH prior to testing regarding what actions are most likely to destroy files. If MDCH does not follow these instructions, and the system must be restored using the backup, MDCH will provide reasonable compensation for restoration time. Contractor will provide the services described, including system backup, defined in the Equipment Location and Services Agreement during the PARE process.

a. Determination of System Readiness

- 1) Prior to the PARE, a committee of three persons will be formed to evaluate the system's performance on a daily basis. The committee will consist of one Contractor representative and two State personnel.
- 2) The PARE will begin on the installation dates when the Contractor certifies that the physical system, directory structure, role structure, and user contact data is installed.



- b. During the PARE:
 - All rerun times resulting from equipment failure and preventive maintenance shall be excluded from the performance hours.
- 1) All reconfiguration and reload time shall be excluded from the performance hours.
- 2) If files are destroyed as a result of a problem with Contractor equipment and must be rebuilt, the time required to rebuild the files will be considered "down-time" for the system.
- 3) If the Contractor requests access to failed equipment and the State refuses, then such maintenance will be deferred to a mutually agreeable time and the intervening time will not count against the PARE.
- 4) A functional benchmark demonstration will be run for the PARE Committee to confirm that the installed system is capable of performing the same functions that were demonstrated. This run must be completed to the satisfaction of the PARE Committee.

3. STANDARD OF PERFORMANCE

- a. The performance period (a period of thirty consecutive calendar days) shall commence on the installation date. It is not required that one thirty day period expire in order for another performance period to begin.
- b. If each component operates at an average level of effectiveness of 95 percent or more for a period of 30 consecutive days from the commencement date of the performance period, it shall be deemed to have met the State's standard of performance period. The State shall notify the Contractor in writing of the successful completion of the performance period. The average effectiveness level is a percentage figure determined by dividing the total operational use time by the total operational use time plus associated down-time. In addition, the equipment shall operate in substantial conformance with the Contractor's published specifications applicable to such equipment on the date of this Agreement. Equipment added by amendment to this contract shall operate in conformance with the Contractor's published specifications applicable to such equipment at the time of such amendment.
- c. During the successful performance period, all rerun time resulting from preventive maintenance time shall be excluded from the performance period hours. All reconfigurations and reload time shall be excluded from the performance hours. Scheduled and equipment failure down-time will be removed from effective performance hours and total performance hours when measuring performance.
- d. During the successful performance period, a minimum of 80 hours of operational use time on each component will be required as a basis for computation of the average effectiveness level. However, in computing the effectiveness level, the actual number of operational use hours shall be used when in excess of the minimum stated above.
- e. No more than one hour will accrue to the performance hours during any one-wall clock hour.
- f. Equipment shall not be accepted by the State and no charges will be paid by the State until the standard of performance is met.



- g. When a system involves on-line machines which are remote to the basic installation, the required effectiveness level shall apply separately to each component in the system.
- h. Promptly upon successful completion of the performance period, the State shall notify the Contractor in writing of acceptance of the equipment and authorize the monthly payments to begin on the first day of the successful performance period.
- i. If successful completion of the performance period is not attained within 30 days of the installation date, the State shall have the option of terminating this Contract, or continuing the performance tests. The State's option to terminate the contract shall remain in effect until such time as a successful completion of the performance period is attained. The Contractor shall be liable for all outbound preparation and shipping costs for contracted items returned under this clause.
- j. The PARE will be complete when the equipment has met the required effectiveness level for the prescribed time period.

I-TT SECURITY

This Contract may require frequent visits to State of Michigan facilities. The Contractor shall ensure that all measures utilized by their firm provide for the security and safety of these buildings. This shall include, but is not limited to, performance of security background checks on all personnel assigned to State of Michigan and how they are performed, what the security check consists of, the name of the company that performs the security checks, use of uniforms and ID badges, etc. If security background checks are performed on staff, bidders shall indicate the name of the company that performs the check as well as provide a document stating that each employee has satisfactorily completed a security check and is suitable for assignment to the State. Upon request by the State, the Contractor shall provide the results of all security background checks.

Upon review of the security measures, the State will decide whether to issue State ID badges to the Contractor's personnel or accept the ID badge issued to personnel by the Contractor.

The State may decide to also perform a security background check. If so, the Contractor will be required to provide to the State a list of all people that will service the State of Michigan, including name and date of birth, social security number of driver license number.

The Contractor and its subcontractors shall comply with the security access requirements of individual State facilities.

I-UU SHIPPING AND SET UP COST ESTIMATE TO RELOCATE EQUIPMENTS TO MICHIGAN, UPON TERMINATION OF THE CONTRACT

The shipping will be at actual cost and the state of Michigan can choose the shipping method and carrier. The installation in a new location will be \$ 23,000.00 per site. De-installation will be \$8,000.00, if performed by Virtual Alert, Inc. Travel costs will be extra per the State of Michigan travel rates.



I-VV PRICE GUARANTEE

Virtual Alert, Inc. shall extend a “price guarantee” not to exceed price schedule under this agreement for additional servers and user licenses, showing volume discounts for each level of license, beyond the contractual period of September 30, 2003. The volume discounts will be as follows:

- List pricing for Full Access (Level 4) licenses = \$495 per user
- List pricing for Limited Access (Level 2+) licenses = \$120 per user
- For the first 3500 cumulative users, 20% discounts
- For the next 1500 users (cumulative total = 5,000), 30% discounts
- For the next 5,000 users (cumulative total = 10,000), 35% discounts
- For the next 10,000 users (cumulative total = 20,000), 40% discounts
- For the next 10,000 users (cumulative total = 30,000), 45% discounts
- For the next 10,000 users (cumulative total = 40,000), 50% discounts
- For the next 10,000 users (cumulative total = 50,000), 55% discounts



SECTION II

WORK STATEMENT

II-A TASKS

Introduction

Michigan Department of Community Health (MDCH) must procure a Health Alert Network (HAN) to facilitate secure, rapid communications with public health planners, emergency responders, and partners. The system must meet the Critical Capacity requirements of Focus Area E of the Centers for Disease Control and Prevention (CDC) Public Health Preparedness and Response for Bioterrorism grant and the updated definition of Focus “E” – specifically, Health Alert Network, Communications and Information Technology. Furthermore, the system must be based on standards to the CDC Grant - Public Health Information Technology Functions and Specifications (for Emergency Preparedness and Bioterrorism) such as Lightweight Directory Access Protocol (LDAP) and Secure Socket Layer (SSL).

Time is of the essence for establishing the Michigan HAN as MDCH is leading Michigan's efforts to protect Michigan's residents from the risk of a smallpox event. The first stage of vaccinations will include approximately 6,000 public health staff and medical providers. A second stage of vaccinations for a substantially larger group that includes public safety and first responders will occur soon after. Finally, a third stage that includes the general public will be completed. MDCH must work in concert with public and private health staff, other state agencies, and federal agencies to ensure timely and effective protection of Michigan's 10 million plus citizens. The Michigan HAN must be in place to facilitate secure, accurate communications regarding this expedited, complex vaccination process. Already, MDCH has faced substantial challenges preparing and coordinating statewide smallpox vaccination plans in collaboration with public and private health staff. The pace and criticality of these coordinated efforts will increase as the vaccinations commence.

1. Secure Web Based Portal

The system shall be accessible to users through a web browser interface in an extranet environment. It shall challenge users for appropriate authentication. The portal shall have the capability to provide information content dynamically with minimal intervention by technology professionals as well as organize content in both static (storage) and dynamic (categorizations) formats. This includes separation of normal documents, News, Announcements, and user-specific alert status, reports and historical information which can all be maintained by non-technical Public Health Professionals through normal browser procedures.

This portal will be used for the collaborative development of protocols, standards, guidance and process and shall separate author and reader roles, as well as support document-specific discussion threads and document management features including document check-in, checkout and version control, at a minimum.



2. Public Health Directory

The system must be able to support an LDAP compliant, role based directory with roles specific to Public Health. This directory will be used for applying “Public Health Role” rights as well as be the primary identification technique for alerts and notifications. This functionality is in addition to traditional “grouping” for security or document publishing/management roles. The Directory shall support contact look-up by public health role exporting/ replication of the Directory with other jurisdictions. The Directory must be extended to control access to all other functionality dependent on user role. A single Directory design must be usable for, and the system must be expandable as, a platform to provide for the integration of other Focus Area solutions, as well as extend access control to other functionality and applications.

The Public Health role-based Public Health Directory shall serve as the authentication and validation directory for logon access and assignment of rights. The fully populated directory may be extensible to serve as a foundation for the NEDSS Public Health Directory element, also.

3. Alerting

The system shall have the capability to send alerts via SMTP messaging (such as email, alphanumeric pagers and wireless devices), telephone and fax, utilizing the Public Health Directory Roles. Public Health non-technical administrators must be able to define the alert-able roles for every role in the directory. Within those parameters, users must be able to flexibly determine which roles they want to send individual alerts. Each alert shall have the capability for an immediate, secure confirmation process with appropriate reporting and auditing. This includes the option for a personal identification number for phone-based alerts. Users must be able to flexibly define the duration of the alert.

Additionally, the system shall support “tiered” support for alerts within specific subgroups – rather than simple lists. The functionality must support the CDC HAN specification for separation of alerts into three priorities – low, medium and high.

Users must be able to easily establish and maintain their own alert profiles. This shall allow users to set multiple profiles for how they will receive a low vs. medium vs. high alert.

4. Collaboration

The system shall have the capability to enable participants to collaborate on documents, including discussion threads directly linked to the documents, and manage the access to the documents based on the role or roles that a user populates. If the users have the security and permission to do so, they shall be able to check in, check out, publish and comment on a document. They also must be able to automatically fax distribute any individual document from the portal.

Additionally, the system shall allow users with appropriate authority to set approval routing required to make changes in a particular folder. The system shall enable multiple types of approval schemes (such as all approvers required, only one approver required, or all approvers in a defined sequence).



The system must be able to perform both simple and complex searching for content on the portal. Users shall be able to “subscribe” to documents, folders, categories and searches. This provides the functionality to “filter” information push so that the user does not have to repeatedly “look” for updated documents or be inundated with list-serve type “broadcasts.” The system must be intelligent in that it does not display documents (either through self-navigation or searches) that the user does not have the proper security or permission to view.

This collaboration component is a key element to the Michigan HAN. As previously stated, MDCH faced a substantial challenge in preparing and coordinating a smallpox vaccination plan that included at a minimum the activities of MDCH, eight regional entities, and 45 local health jurisdictions. These plans had to be completed in less than 30 days. It is unlikely that responses to events that are necessitating smallpox vaccinations will have the luxury of a 30-day planning period.

5. Administration

Given the nature of the Michigan HAN, non-technical Public Health Administrators must be able to administer the vast majority of functionality within the systems as well as users, roles and permissions via a web browser interface in an extranet environment. This includes:

- Add new Public Health roles (including organization units) and modify existing roles and organization units.
- Define what other roles the new role has the ability to notify/alert.
- Add users, assign users to roles, reset user passwords and PINs, modify users' contact information, and modify the way that a user receives alerts.
- Maintain content folders and categories.
- Maintain the home page of the portal including posting of informational content to “global” or “portal-wide” areas
- Easily identify who is a member of the groups, as well as go to a group and see a list of members.
- Assign folder permissions to limit the use and ability to access information on sensitive folders.
- Establish “permission groups” for document access, as well as modify permission groups.
- Audit all alerts and confirmations, with the ability to sort/search for specific user-defined parameters.
- Maintain a single user profile entry within the Public Health Directory, which controls their information in the directory, their profile within the underlying alerting engine, and their permissions for all of the collaboration functionality.
- Pull reports of alert logs, alert confirmations, folder permissions, document check out log, document history, modified documents, and a report of the total number



of documents on the system so that administrators can manage the system.

- Individual users must be able to maintain their contact information, dictate how they receive different levels of alerts and notifications, and update/change their password.
- The system must also be able to delegate administration of the Public Health Directory out to other users (such as local officials) while still controlling who and what those delegated administrators have the authority to control within the system.

6. Software, Software Maintenance, and Hardware

The Contractor shall provide software that meets the above-specified requirements and provide a Software License Agreement; provide software maintenance through September 30, 2003 with option for renewal with an associated Software Maintenance Agreement; and the hardware required to operate the system at a primary and separate back-up location. The State of Michigan will have full ownership of the hardware and the option to re-locate the hardware. Additionally, the State of Michigan will have rights in accordance with the Software License Agreement to continue use of the software without renewal of the Software Maintenance Agreement.

7. Associated Consulting, Training, Installation, and Hosting Services

Contractor shall also provide the following services: pre-installation consulting to set the business rules that will govern the setup and usage of the system; training on the system; and system installation at hosted primary and backup sites as specified in the Equipment Location and Services Agreement.



II-B OBJECTIVE

1. DELIVERABLE SCHEDULE

The period of performance for this contract will be from March 17, 2003 through September 30, 2003. The Contractor will provide hardware, software, software maintenance, pre-installation consultation and training, and hosting services at a primary and backup site in accordance with the schedule provided below. The State of Michigan understands that timely completion of several deliverables is dependent on timely input from State staff regarding business rules and contacts.

	Brief Description	Deliverable Date From the date the Contract is executed
Work Plan	Schedule with tasks, staffing level, and completion dates	14
Standard Training Materials	1 electronic copy and 3 hardcopies of standard training materials	14
Business Rule Development Consultation	2 five-day site visits in Lansing, MI to develop business rules with telephone consultation as required between site visits	Visit 1 – 21 days Visit 2 – 42 days
Hardware, Hardware Installation, Software, Software Installation	Purchase and install hardware and system software at approved co-location sites	56 days
Performance and Reliability Evaluation (PARE) Support	Support system testing and acceptance for PARE period	90 days
Training	5 consecutive days of training in Lansing, MI with training materials for participants. Currently expect 2 two-day classes with approximately 25 participants and 1 one-day class with 25 participants.	120 days
Co-location Services	Hosting services at approved primary and backup site from start of PARE period through September 30, 2003 in accordance with Equipment Location and Services Agreement.	September 30, 2003
Software Maintenance	System software maintenance as established in Software Maintenance Agreement.	September 30, 2003



2. Payment Schedule

Payment will be initiated upon receipt of invoice according to the following schedule of activities and only after acceptance and approval of deliverables.

Activity/Deliverable	Items Covered	Payment
Contract Initiation	<ul style="list-style-type: none"> • Hardware • Technical Installation • Co-location Setup • 3 months co-location service at 2 sites including PRI line setup and operation • Long distance deposit for 3 months @ \$500/month • Pre-Installation Package + travel at cost using State Travel Regulation pricing • 80% of Server and User License Costs with 481 Level 4 licenses and 1386 Level 2+ licenses (optional user licenses addressed below) 	<p>\$94,650</p> <p>\$29,460</p> <p>\$6,000</p> <p>\$45,830¹ + long distance cost</p> <p>\$1500</p> <p>\$34,600+travel</p> <p>\$437,000</p> <p>Total \$649,040 + travel + long distance</p>
Performance and Reliability Evaluation (PARE) <i>Completion and Acceptance</i>	<ul style="list-style-type: none"> • Software Maintenance through September 30, 2003 (Assumes March 15 contract date so 6½ months of maintenance) • 20% Balance of Server and User License Costs 	<p>\$64,800</p> <p>\$108,692</p> <p>Total \$173,492</p>
Long Distance First 3	<ul style="list-style-type: none"> • Long distance services at cost 	Long Distance at Cost less

¹ Assumes 0.5 baseline and 2.5 Mbps burstable Internet access at \$750 per month per site but to be billed at cost as presented in detailed price proposal. Also includes PRI lines at estimated cost of \$555 per month at Austin, TX site and \$555 per month at Sacramento, CA site with \$700 set up fee per site.



Activity/Deliverable	Items Covered	Payment
Months	for initial 3 months of co-location	\$1500 deposit
Co-location Service and Long Distance after Initial 3 months	<ul style="list-style-type: none"> Co-location monthly fee billed monthly for primary and backup sight includes hosting and PRI line plus long distance Long distance service at cost Service may be canceled with 30 days notice with option for renewal after September 30, 2003 	\$14,810 ² per month + long distance at cost less remaining deposit
Training	<ul style="list-style-type: none"> 5 consecutive days of training in Lansing, MI plus travel at State Travel Regulation pricing 	\$10,000 plus travel costs
Optional licenses	<ul style="list-style-type: none"> Up to 150 additional Level 4 licenses at \$495 and 1070 Level 2+ licenses at \$120 less a 20% discount Maintenance at 18% on undiscounted price prorated through September 30, 2003 	Payment due upon exercising option.

*Third-party software to be provided by State of Michigan

C PROJECT CONTROL AND REPORTS

1. Project Control

- a. The Contractor will carry out this project under the direction and control of the Contract Administrator (See I-D).
- b. Although there will be continuous liaison with the Contractor team, the client agency's project director will meet periodically with the Contractor's project manager for the purpose of reviewing progress and providing necessary guidance to the Contractor in solving problems which arise.
- c. The Contractor will submit brief written summaries of progress, as required by the Contract Administrator, which outline the work accomplished during the reporting period; work to be accomplished during the subsequent reporting period; problems, real or anticipated, which should be brought to the attention of the client agency's project director; and notification of any significant deviation from previously agreed-upon work plans.

² Assumes 0.5 baseline and 2.5 Mbps burstable Internet access at \$750 per month per site but to be billed at cost as presented in detailed price proposal. Also includes PRI lines at \$555 per month per site.



I-D PRICE PROPOSAL

All prices/rates quoted in the Contractors proposal will be firm for the duration of this Contract.
No price changes will be permitted.



APPENDIX 1 EXECUTIVE SUMMARY



MICHIGAN

Public Health Preparedness and Response for Bioterrorism
Supplemental Funding Request

To

The Centers for Disease Control and Prevention

And

Bioterrorism Hospital Preparedness Program
To
Health Resources and Services Administration

Executive Summary

April 2002



Introduction

On January 10, 2002 President Bush signed appropriations acts intended to develop comprehensive bioterrorism preparedness plans, upgrade infectious disease surveillance and investigation, enhance the readiness of hospital systems to deal with large numbers of casualties, expand public health laboratory and communications capacities, and improve connectivity between hospitals, and local and state health departments to enhance disease reporting.

Later that same month, Health and Human Services (HHS) Secretary Tommy G. Thompson sent letters to governors detailing how much each state would receive of this \$1.1 billion.

“We’re putting money in the hands of states and local communities so they can start building strong public health systems for responding to a bioterrorism attack,” Secretary Thompson said. “These funds are just the start of our efforts to help states and communities build up their core public health capabilities. We must do everything we can to ensure that America’s ability to deal with bioterrorism is as strong as possible.”

The funding to states and communities is divided into three parts. The first portion comes from the Centers for Disease Control and Prevention (CDC) and is targeted to support bioterrorism, infectious diseases, and public health emergency preparedness activities statewide. For Michigan the amount from CDC is \$27.1 million.

The Health Resources and Services Administration (HRSA) is providing the second portion of funding, which is to be used by states to create regional hospital plans to respond in the event of a bioterrorism attack. For Michigan the amount from HRSA is \$4.1 million.

The HHS Office of Emergency Preparedness, through support of the Metropolitan Medical Response System (MMRS), provides the third portion of funds. MMRS contracts are especially aimed at improving local jurisdictions’ ability to respond to the possible release of a chemical or biological disease agent, but also to serve to improve local response to any event involving mass casualties. For Michigan the cities and amount received Warren - \$400,000, and Grand Rapids - \$200,000. Grand Rapids and Detroit had received previous funding as well.

Both the CDC and HRSA awards required states to submit applications. The CDC award is a supplemental award to an existing Public Health Preparedness and Response for Bioterrorism cooperative agreement project. The HRSA award is a new cooperative agreement.

Governor John Engler has strongly supported and endorsed both grant applications. “This crucial federal funding and our comprehensive strategy will enable us to continue to prepare for and quickly respond to the threat of bioterrorism in Michigan, said Engler. While we have accomplished a great deal in our preparedness efforts previously, this funding will allow us to build on our existing infrastructure to protect our communities.”

Over the last several years, Michigan and other states have received smaller funding awards from the CDC. This prior funding has been used to increase the ability to respond to acts of bioterrorism across the entire state, with focus on coordinating emergency management



activities, enhancing disease detection and reporting, improving biological and chemical laboratory capacity, and enhancing Michigan's health alert network.

“Thanks to the cooperative and significant planning efforts that have gone into our work on this issue over the years, Michigan is in a much better position to aggressively pursue this considerably greater federal funding,” said Michigan Department of Community Health Director, James K. Haveman, Jr. Working cooperatively on this issue with the Michigan State Police, FBI, local health departments, Michigan National Guard, Emergency Medical Services representatives, Poison Control Centers, many physicians, hospitals and other partners has allowed us to promptly develop and submit these important grant proposals.”

The CDC application addresses seven focus areas. One focus area (Focus Area D) titled, Laboratory Capacity – Chemical is not part of the supplemental award but is funded as part of the original award, with increased funding expected next year. The focus areas and their titles are:

FOCUS AREA A – Preparedness Planning and Readiness Assessment

FOCUS AREA B – Surveillance and Epidemiology Capacity

FOCUS AREA C – Laboratory Capacity – Biologic Agents

FOCUS AREA E – Health Alert Network/Communications and Information Technology

FOCUS AREA F – Communicating Health Risks and Health Information Dissemination

FOCUS AREA G – Education and Training

The HRSA application addresses two phases. The first phase is for Needs Assessment, Planning and Initial Implementation, and the second phase is for Implementation.

Summaries for the CDC focus areas and the HRSA phases follow.



CDC Cooperative Agreement

Focus Area A: Preparedness and Planning

The events of 9/11, concerns of anthrax exposure, and the introduction of West Nile virus in Michigan, highlight the need to build state and local public health infrastructure to plan and respond to public health emergencies with rapid coordination and communication between public and private partners.

Funding under this cooperative agreement will build the infrastructure at the state and local level for the development of local, regional and statewide plans, and consequent exercising of those plans. Development of integrated inter-agency plans will require the dedication of resources to develop networks and relationships to assure a collaborative planning process. While the end product results in a resourceful planning document, it is the process itself that develops the infrastructure to respond efficiently and effectively to public health emergencies.

Under current Michigan Emergency Management Plan requirements, the Michigan Department of Community Health (MDCH) is tasked with protecting the health of Michigan's citizens and coordinating the allocation of medications and medical services essential to the public health during a state emergency, including the receipt and distribution of supplies from the CDC National Pharmaceutical Stockpile. However, command and control, planning, logistical emergency management support, and security from the Michigan State Police are essential to these efforts. All planning activities will be closely integrated within the existing state and local emergency management infrastructure. Funding proposals to support preparedness and planning in Michigan include:

- Development of a Michigan Medical Advisory Committee to lead Michigan's public health preparedness effort, along with needed subcommittees and workgroups
- Assessment of local public health capabilities and capacities to respond to public health emergencies
- Development of state and local public health emergency preparedness response plans
- Comprehensive assessment of credentialing and licensure of medical volunteers, and exploration of local public health Mutual Aid Compacts
- Development of state and regional national pharmaceutical stockpile receipt and distribution plans
- Coordination of medical response efforts with local public health, private health care providers, and other federally funded programs including hospital and Metropolitan Medical Response System bioterrorism planning
- Coordination of public health emergency planning with tribal health centers and boarding states and countries



Focus Area B: Surveillance and Epidemiology

The main purposes of this focus are to enhance, design, and develop systems for rapid detection of unusual outbreaks of illness that may be the result of bioterrorism, other outbreaks of infectious disease, and other public health threats and emergencies; to assist state and local health departments in establishing expanded epidemiologic capacity to investigate and mitigate such outbreaks of illness.

Public Health Surveillance and Detection Capacities

The successful development of a broad and alert disease surveillance system for Michigan will involve the implementation of a new system that uses new and existing computer technologies. The new system will allow public health staff the ability to:

- Capture disease reports through a secure web page and transmit information between MDCH and local health departments (LHDs).
- Perform analyses; prepare standard and *ad hoc* reports, and present geographic data using commonly available software tools at both LHDs and MDCH
- Comply with CDC National Electronic Disease Surveillance System (NEDSS) requirements.
- Capture laboratory data electronically.
- Provide on-going support, education and marketing to ensure public and private provider participation.
- Ensure the system complies with Health Insurance Portability and Accountability Act (HIPAA) requirements and other nationally mandated or generally accepted electronic data interchange and data standards.

In addition to upgrading the electronic capabilities of Michigan's surveillance system, efforts will also focus on expanding and improving our ability to detect changes in disease patterns through a network of disease surveillance projects based on sets of symptoms, known as syndromic surveillance.

Public Health Epidemiologic Investigation and Response Capacities

An effective epidemiologic plan in Michigan will be comprised of a comprehensive approach consisting of state, regional and available local epidemiologists, epidemiology response teams and an effective communication network.

To effectively address the need for epidemiologic capacity, MDCH has worked with partners in local health jurisdictions, the medical community and academia in developing a plan:



Regional Epidemiologists

- Eight regional epidemiologists with coverage areas corresponding to the eight emergency management districts identified by the Michigan State Police.
- They will provide of analytical assistance to the local health departments, coordination of response efforts, and a communications link to MDCH and neighboring health jurisdictions.
- This will participate in exercising around, planning for and responding to public health emergencies at the state and regional level.

Increased state-level epidemiologic assistance

- Hiring of state-based staff positions with expertise in infectious diseases and environmental epidemiology, who would be available for consultation on a statewide to local emergency management, and other state agencies.
- Assist in developing training for other state and local public health staff, healthcare providers, and local law enforcement/first responders in conjunction with Focus Area G.
- Providing financial assistance to local health departments.

Development of epidemiology response and investigation teams to assist with public health emergencies.

- Membership in these teams will include representatives from several disciplines inside and outside of the public health field in order to address the diverse array of potential public health emergencies that may arise.
- Members of these teams will receive enhanced training and equipment.
- These teams coordinate response with regional epidemiologists, local public health agencies, and local emergency management staff.

Assessment of food and water production facilities in the state

- Vulnerability assessments of these production facilities in Michigan will be conducted in collaboration with appropriate state agencies to ensure protection of resources.
- Coordination with academia on assessment approach and coordination with appropriate state agencies on the sharing of information regarding further assessments of the vulnerability of these resources will also be key components.



Focus Area C: Laboratory Capacity – Biologic Agents

The rapid isolation and identification of a biological agent associated with bioterrorism (BT) will directly impact the number of casualties and fatalities associated with the event and will guide disease control efforts. A large measure of this diagnostic responsibility will fall on hospital and public health laboratories. To facilitate this process laboratories in Michigan have enrolled in the Laboratory Response Network (LRN) for Bioterrorism. LRN laboratories are divided into four levels, A – D.

- Hospital and clinical microbiology laboratories are designated Level A and will screen all patient samples for the agents of bioterrorism, perform basic testing and rapidly refer them to a higher-level lab for confirmation.
- Public health labs that isolate, identify, confirm the identification of Level A referrals, and may perform antibiotic susceptibility testing on agents are Level B labs. The laboratories are currently located in Grand Rapids, Kalamazoo, Saginaw, Lansing, Houghton, and Detroit.
- The Michigan Department of Community Health Bureau of Laboratories (MDCH BOL) in Lansing is a Level C facility that can perform rapid tests for identification, test for botulinum toxin, test environmental samples and apply advanced molecular techniques to these agents.
- The Centers for Disease Control and Prevention (CDC) in Atlanta is the Level D lab and will provide technical expertise, confirm the identifications made by Level B and C labs, develop testing methods, and examine BT isolates for genetic manipulation.

Funding from this focus area will go to four primary areas: 1) to enhance and expand the capacity of public health laboratories to respond to bioterrorism and other public health emergencies; 2) to provide training for hospital clinical laboratories (Level A) in the recognition of the agents of bioterrorism; 3) to improve communications between all levels of laboratories and their partners in law enforcement and emergency management; and 4) rapid specimen transport between facilities.

The events following September 11 have shown that public health laboratories must be capable of a sustainable round-the-clock response. MDCH BOL will add more scientists to its laboratory staff. These individuals will be trained to perform testing for the agents of bioterrorism associated either with human or environmental samples. Combined with existing staff, the BOL will be capable of providing laboratory testing 24 x 7 in emergency situations. The BOL will enhance capabilities by adding additional instrumentation for rapid molecular testing and renovating existing laboratory space to safely work with highly pathogenic organisms. Other public health laboratories in Michigan will receive funding to improve security and provide expanded emergency services. A sixth Level B laboratory will also be added in Southeastern Michigan to increase laboratory capacity and cut response time. An additional Level B laboratory will receive training and join the Lansing lab in processing environmental samples e.g.,(white powders).

The laboratory training coordinator has provided in-service training on testing of BT agents for almost 90% of the clinical microbiology laboratories in the state. A manual of standardized procedures for Level A labs is presented to each lab when they receive training. The training coordinator will continue to train hospital laboratories about the agents of bioterrorism and to



provide annual training about new agents of concern. The procedure manual will be updated regularly and distributed to laboratories in an electronic format. MDCH will offer a series of workshops for Level A laboratories, so that hospital laboratorians will have the opportunity to have a first-hand working knowledge of organisms that are rarely seen in most laboratories.

Timely communication of critical information and test results to hospitals, emergency responders, law enforcement and other public health agencies is important. Test results and important information is sent to Level A laboratories and other partners sent via fax either through the laboratory information system (LIS) or a broadcast network. Such a system could easily be compromised during an emergency. Redundant communication capabilities including web based reporting of results, use of 800MHz radios, pagers, e-mail servers, and cellular telephones will be added in an effort to maintain close and uninterrupted communications.

Rapid identification of the agents of bioterrorism depends on the ability of hospital labs to presumptively identify the agent and the ability of a public health laboratory to receive and confirm the identification in a timely manner. Currently there is no coordinated system to transport specimens between hospital and public health labs. MDCH will develop a statewide courier system to transport critical and routine samples from hospitals and local health departments to the state and regional public health laboratories.

While these enhancements will markedly improve the ability of laboratories in Michigan to respond to a bioterrorism event, they also strengthen the infrastructure of public health. The surge capacity obtained from added laboratory staff, the ability to transport critical specimens between laboratories, and improved communications capabilities are key to the response for any public health emergency.

Focus Area E – Health Alert Network/Communications and Information Technology

The primary focus of the Health Alert Network (HAN) is to ensure effective communications connectivity among public health departments, healthcare organizations, law enforcement organizations, public officials, and other as evidenced by: a) continuous, high speed connectivity to the Internet; b) routine use of e-mail for notification of alerts and other critical communication; and c) a directory of public health participants (including primary clinical personnel), their roles, and contact information covering all jurisdictions.

This focus area will also ensure a method of emergency communication for participants in public health emergency response system that is fully redundant with e-mail.

Finally, this focus area will ensure the ongoing protection of critical data and information systems and capabilities for continuity of operations. This includes secure electronic exchange of clinical, laboratory, environmental, and other public health information in standard formats between the computer systems of public health partners. Achieve this capacity according to the relevant information technology functions and specifications.



Where connectivity is concerned, we will first hire a source to evaluate what the connectivity is in all counties in Michigan. Using this analysis we will determine how best we can implement technologies such as broadcast fax, bi-directional text paging, two-way 800 MHz radio communications and the use of the Internet both for e-mail and secured web site applications. Also included in this process is the design of the directory of public health participants.

Expanding on the communications connectivity capacity we must focus on the bi-directional nature of the communications to the health alert community. We must be certain that the appropriate party receives a message sent. Also, we must be certain that the correct person receives the correct message. There are cases where not everyone will receive the same message. This will be a combination of the directory telling us the role of each party and the communications system to define how we contact them.

Tightly tied to both of these capacities is our ability to ensure that the HAN is running when it is needed. This is a matter of capacity as well as the ability to withstand an attack and to recognize that one is under way. The system must be alert to detect an attack and hardened to ensure that it can withstand it. Should a disaster occur, we must have the ability to quickly reestablish our operations and the operations of the business units. This means that both they and we must have a business process analysis that includes disaster planning. Finally, data integrity must be assured. We must be able to understand what good data are and what bad data look like. The system must be sensitive to both.

Focus Area F: Risk Communication and Health Information Dissemination

Under this focus area, MDCH and local health departments will develop capacity and infrastructure to assure that citizens are provided with timely and accurate information during a public health threat or emergency. One of the lessons learned last year, in Michigan and nationally, from the anthrax event was that public health agencies at all governmental levels need to have detailed, coordinated plans for how to communicate with the public during a public health crisis. Effective crisis communication must be based on the most current science and on state-of-the art in risk communication strategies, must be communicated through an established chain-of-command, and must be delivered by highly trained spokespersons.

The MDCH plan to accomplish this goal includes three components: State-wide needs assessment of current capacity for crisis public health communications; development of agency risk communication plans based on best practices in risk communication and sound medical science; and development of a cadre of trained spokespersons.

Needs assessment: The current capacities and organizational structures around risk communication for public health emergencies will be assessed at MDCH and other state agencies that would most likely be involved in a public health emergency and at all 45 local public health agencies. The assessment will obtain information on each agency's "chain of command" for communicating with the public during an emergency; current communications staffing/resources and their limitations, including the internet, printed media, and expertise in design and execution of materials; and plans for communication in an event that would require evacuation from the



office. Specific infrastructure and resource needs will be identified by each respondent, which are relevant for communications with the public about health emergencies. Participating state and local agency will receive a report with specific findings and recommendations from the assessment. Each agency will be asked to prepare a response and to indicate its plan to implement recommendations. At the end of the funding period, each agency will be surveyed to determine the success of each agency's implementation of their plans.

Best practices in risk communication and plan development: MDCH will partner with one or more of the state universities and appropriate voluntary/non-profit organizations to obtain the services of experts in health risk communication, medicine, toxicology, epidemiology, food safety, water safety, veterinary health, and others. Deliverables under these agreements will include the following:

- Provide a report with recommendations and an implementation plan for reaching the public and special populations through effective channels of communication based on a review of the literature on state-of-the-art risk communication strategies and resources.
- Develop and maintain a clearinghouse/library of best practices in health risk communication, particularly as they pertain to bioterrorism and public health emergencies.
- Develop and maintain a clearinghouse of scientific literature on clinical, toxicological, and epidemiologic aspects of potential agents of bioterrorism and chemical agents.
- Develop a risk communication/crisis communication curriculum for train-the-trainer, utilizing best practices information and the scientific clearinghouse.
- Develop a Michigan-specific model plan for risk communication to address public health emergencies in a state agency or local health department

MDCH will ensure on-going dissemination of information in the clearinghouses for risk communication best practices and scientific literature.

MDCH will use the model risk communication program developed by the contractor to develop a detailed risk communication plan for the agency. The model plan will also be used by other potentially affected state agencies and all local health departments to develop their agencies' plans.

Trained public health spokespersons: The training program developed by the contractor above will be administered to appropriate staff within MDCH, in other key state agencies, including the Governor's office, and from key partnering agencies (e.g. American Red Cross, Michigan Hospital Association, Michigan College of Emergency Physicians, Michigan Infectious Disease Society, Michigan Society of Infection Control) under Focus Area G. Each local health department will designate a key staff to be the agency's lead person in communications with the public and will identify the lead governmental official(s) in their jurisdiction who would be the official governmental spokesperson(s) as part of their risk communication plan. These individuals will be trained using the curriculum developed by the contractor. In addition, each local health department will convene a committee of community and agency representatives to serve as advisors, community liaisons, and opinion leaders for bioterrorism and public health response. Physicians, emergency response personnel, the county director for emergency response, police, fire, American Red Cross, United Way, community leaders (e.g. clergy) and others should be represented. They too will be trained and will be expected to serve as a "speakers bureau" when needed.



FOCUS AREA G: Education & Training

This focus area concentrates on ensuring the delivery of appropriate education and training to key public health professionals, infectious disease specialists, emergency department personnel, and other healthcare providers in preparedness for and response to bioterrorism, other infectious disease outbreaks, and other public health threats and emergencies, either directly or through the use (where possible) of existing curricula and other sources, including schools of public health and medicine, academic health centers, CDC training networks, and other providers.

The Michigan Department of Community Health has assessed training needs and capacities and provided training in several of the important areas listed above. These activities have impacted some groups strongly; others on a preliminary or partial basis, and some groups remain largely unassessed and untrained. Existing capacity is strongest in the epidemiology and laboratory areas where training resources for clinicians and laboratorians have been developed and made available over the past two years -- and weakest at the community level and in terms of coordinated approaches to ongoing training using efficacious methods.

The need for coordinated approaches to assessment of need and capacity, and to training development and implementation, is generally acknowledged in this application. Determination of the most efficacious and appropriate training methods and channels for access to training is also an acknowledged need; this is true in strong capacity areas as well as weak ones, since the strong capacity areas already have tried a variety of methods and channels and see the need for further experimentation, evaluation, and resource identification. Across the Focus Areas, to varying degrees, the coordinated extension of assessment and uniform training to the critical professional groups at the local level is seen as inadequate at present.

Activities aimed at improving training capacities must be coordinated with the other activities taking place in Focus Areas A-F, and with programs of other major entities involved in bioterrorism response. Coordination must occur in terms of the timing and targeting of assessment and training activities, as well as their content. Education and training activities must, then, be scheduled for parallel-processing, so that assessment with respect to target groups and tasks where need is great, will not delay the implementation of training tools and access channels for target groups and tasks much closer to full compliance.

Throughout the project period, education and training assessment, planning, and implementation activities will be coordinated in terms of timing and targets with activities related to all the Focus Areas. In addition, if Focus Areas A-F identify training needs as they conduct assessment and planning activities, the Focus Area G Education & Training Workgroup will collaborate with staff from these Focus Areas to plan and implement assessment and/or training for the identified target groups, using appropriate providers of assessment, education and training, and efficacious modes of access to training.

- Prepare timeline to assess training needs, with special emphasis on emergency department personnel, infectious disease specialists, public health staff, and other healthcare providers. This assessment will be planned to utilize recent information from the other Focus Areas, so that target groups whose needs have already been assessed and largely met will be assessed only with respect to retraining needs, preferred channels for delivery of training, and perceived gaps. Target groups who are acknowledged to be not assessed recently with respect to needs and capacities



will be more intensively assessed on all aspects of need, capacities, previous training, gaps in training, and preferred channels for delivery of training.

- Assess existing capacity to conduct training needs assessment and planning for public health and private professionals, and to provide access to training in bioterrorism, other infectious disease outbreaks, and other public health threats and emergencies. This assessment of capacity will be conducted in conjunction with the assessment of training needs. The assessment data will be analyzed in conjunction with existing information resources; a plan for improvements will be developed and implemented as funding permits.
- Develop an ongoing plan for meeting training needs through multiple sources. Using analyses, information and Interim Plans from Assessment of Training Needs and Capacities (above), and identified needs of Focus Areas A-F, develop Training Plan to meet training needs through (as appropriate) utilization of existing resources, provision of additional resources, and more efficacious access channels and methods, including distance-learning technologies. Periodically reassess the extent to which training needs are met, and revise plan.
- Develop the capacity at the state and/or local public health agency to facilitate or provide education and training sessions and services on bioterrorism, other infectious disease outbreaks, and other public health threats and emergencies. Utilizing existing and new resources, the Training Plan will be implemented to include a Distance Learning Network, electronic libraries, dissemination and management of curricula as interactive/streaming video, placement of video-conferencing equipment in selected local health department facilities, and enhancement of local computing, Internet, and communications systems for training.
- Develop formal partnerships with schools of public health and medicine, other academic institutions, and other organizations for the provision of education and training. Identify existing formal partnerships and additional needed partnerships; coordinate with law enforcement, fire department, hospitals and emergency management systems to identify their training resources; prioritize and coordinate formal partnerships for provision of education and training. Implement new partnerships, using the communication resources of existing organizations and universities to structure these relationships. Periodically reassess and revise.
- Ensure educational expertise and review of training program content & curricula by: a) developing/providing training for a Speakers' Bureau; b) providing training in core public health skills to program staff; and c) supporting costs (travel and course fees) for training critical program staff using existing courses. Using results of Training and Capacities Assessment, plan and conduct assessment of needed education expertise of Training Program Staff; analyze data and make recommendations on education needs of Training Program Staff. Develop, implement, and periodically reassess a plan for a) a Speakers' Bureau, with training for Speakers to improve educational expertise of Training Program Staff, b) provision of training in core public health skills to program staff, and c) support of costs of selecting and training critical program staff using existing courses.



HRSA Cooperative Agreement

The Need

The terrorist attacks of September 11, 2001, and the subsequent intentional release of anthrax, have focused attention on the ability of the public health and health care systems, including hospital and emergency medical services (EMS) to respond to bioterrorist events. These events highlighted the need for improved preparations by hospitals, community clinicians and EMS systems to respond to biological attacks and other public health emergencies.

Hospitals, outpatient care providers and EMS personnel face the challenge of becoming trained and prepared to respond to biological mass casualties, whether they present in large numbers acutely or more insidiously over time. While generally well prepared to respond to routine emergencies and minor epidemics, they may lack the plans, resources and infrastructure to respond to the new challenges posed by biological terrorist acts. A sudden influx of huge numbers of sick or contaminated patients from such an attack could completely overwhelm the medical system.

Federal Response

The \$4 million available from HRSA is for the development and implementation of regional plans and other efforts to improve the capacity of hospitals, their emergency departments, EMS systems and other collaborating health care entities to respond to incidents requiring mass immunization, treatment, isolation and quarantine in the aftermath of bioterrorism or other outbreaks of infectious disease. The funds will also be used to improve the communication between hospitals and EMS units, and local and state health departments to enhance disease reporting. This will also improve hospital and medical system capacity for nonterrorist epidemics of rare diseases.

Organization of Michigan Efforts

The HRSA funds will support needed additional hospital and EMS system improvements as part of an overall effort to improve Michigan's capacity to respond to bioterrorism. Bioterrorism activities by hospitals and EMS will be coordinated with related efforts by the state and local health departments to develop comprehensive bioterrorism preparedness plans, upgrade infectious disease surveillance and investigation, and increase communications capacities.

The HRSA funding is being allocated in two phases. Phase 1 funds of \$807,000 were awarded in April 2002 and an application for an additional \$3,280,170 under Phase 2 was submitted to HRSA on April 12, 2002. The Phase 2 award is expected in late May. Under Phase 1 the Department will appoint a Bioterrorism Hospital Preparedness Coordinator and a Project Medical Director. A Bioterrorism Hospital Preparedness Planning Committee composed of experts in hospitals, emergency medical services (EMS), public health, laboratories and infection control has also been convened as part of the Michigan plan. The Hospital Preparedness Planning Committee has been meeting regularly since March to advise the Department on additional steps to be taken under the HRSA grant.

Future Activities



Implementation of the HRSA Agreement will involve four areas:

1. Development of a statewide assessment of the current capacity of hospitals, EMS responders and other health care providers to respond to the threat of bioterrorism. This assessment will be integrated with other statewide assessments under the CDC grants and will guide future funding decisions for local and regional projects;
2. Technical support for hospitals and the emergency medical control authorities that oversee local emergency medical operations. This support will include the development of Planning and Response Guidebooks for both hospitals and the local emergency medical control authorities and a statewide conference to be held in the summer of 2002;
3. Financial support for hospital and EMS capacity improvement projects. Funds will be made available to hospitals and medical control authorities to begin the assist them with planning and implementation of activities designed to address identified needs.
4. Development of a regional hospital and medical services plan in each of the 8 Michigan State Police Emergency Management Districts. This will include the appointment of a regional coordinator to oversee regional needs assessments, plan development, capacity enhancement and coordination with public health, emergency management and other response agencies at the regional level. Regional plans will include:
 - Epidemic planning for events, which may involve more than 500 patients in a community or region
 - Plans for the acquisition, security and distribution of medications and vaccines
 - Plans for personnel protection, quarantine and decontamination
 - Plans to assure dependable communication and coordination of information
 - Bioterrorism disaster drills

Expected Outcomes The outcomes of this effort will be:

- Improved preparedness to respond to public health emergencies, including those resulting from terrorist actions by Michigan hospitals and EMS systems.
- A statewide assessment that identifies the hospital, EMS and health system capacities that need improvement in order to better respond to bioterrorism
- Capacity upgrades for hospitals, medical control authorities and other health care entities to meet identified needs and improve their ability to respond to biological events. These might involve training, equipment, surveillance, medical supply or communications upgrades.
- Regional Hospital and EMS Response Plans to create a multi-tiered system to triage, isolate, treat, stabilize and refer multiple casualties of a bioterrorist incident. The regional plans will also assure communication and coordination with the public health, law enforcement and emergency management resources that respond to a bioterrorist attack.

APPENDIX 2 TECHNICAL PROPOSAL



APPENDIX 2(a) VIRTUAL ALERT BUSINESS BACKGROUND



2. (a) VIRTUAL ALERT BUSINESS BACKGROUND

In 1997, members of Virtual Alert implemented messaging and collaboration systems for the California Department of Health Services (CDHS). This team continued to provide services to CDHS in many areas including web services, messaging, systems management and enterprise architecture. Through this work, the team developed a broad background in the many programs that encompass Public Health. This culminated in the development of California's first web-based Public Health information delivery system, for the County Medical Services Program.

This team was first contracted to develop a proof-of-concept of a bioterrorism portal and alert system in September 2000. This engagement resulted in the California RHEACTS (Rapid Health Electronic Alert Communication and Training System) proof-of-concept from Common-Off-The-Shelf (COTS) software including Microsoft Windows, Exchange and SQL Server. A subsequent contract allowed RHEACTS to develop into a pilot and integrate the services of Microsoft SharePoint Portal Server.

It was during this second phase of the RHEACTS project that the team elected to formalize the various research projects into a unified platform for Public Health. The final pieces of the puzzle were delivered during the CDC NEDSS Conference in April 2001, where various HAN and NEDSS efforts were discussed. Based on its innovative success, California was asked to demo RHEACTS. The team assisted in the successful demo, which was attended by more than ten states.

Shortly after the conference, the Public Health platform for services was defined in order to provide Public Health with a long-term platform that simultaneously addressed a number of issues, including:

- The multiple technical goals
- Funding – make the best use of limited available funds
- Competitive Government Contracting – make it viable for other vendors to develop on top of the platform and not exclude proprietary systems

The team moved forward with the development of the platform and was also awarded contracts by the County of Los Angeles and State of Arizona to implement bioterrorism systems comparable to RHEACTS. The team also received contracts to replace an IBM Websphere/ GoDomino/ DB2-based pilot for the CDHS Microbial Disease Laboratory system with one that is based on Microsoft technologies; to implement the California Electronic Laboratory Disease Alert and Report (CELDAR) system and an Integrated Data Repository for the non-profit Public Health Foundation.

The California and Los Angeles County systems were demonstrated at the Public Health Informatics Conference, in Columbus, OH, at the request of the CDC.



After the events of 9/11/01, the interest in the bioterrorism system and the Public Health Platform increased significantly and a large number of state and local PHJs were expressing interest in the team's offerings. Additionally, the team realized that the various applications of the Public Health Platform (HAN, NEDSS, LRN, Epi-X, etc.) need the capability to leverage the same core services and to inter-operate—both within a jurisdiction and across jurisdictions—if they are to successfully serve the purpose of protecting the public.

The team realized that the only way to serve the tremendous demand, and deliver solutions that would actually achieve their Public Health missions (and technical goals) was to develop a truly productized software solution. They also realized that one-off custom solutions would be more costly for clients to implement and support, and would have great difficulty in meeting the goals of inter-operability. Virtual Alert was thus formed to develop, market, implement and support these Public Health offerings as Common-of-the-Shelf-Software “package products”.

The first product, BioTerrorism Readiness Suite (BTRS) was developed to serve the CDC vision of an integrated Public Health Information Platform. As the HAN requirements were the most urgent at the time, early development focused on ensuring that BTRS meets all HAN requirements. Since its formation, Virtual Alert has secured the Commonwealth of Massachusetts, the State of Washington and the State of Hawaii as BTRS clients. As proof of the continuing quality of BTRS, the State of California has also contracted to upgrade from the RHEACTS prototype (described above) to the Virtual Alert BTRS product. At least five other states are in the process of purchasing BTRS. Other clients on the early prototype systems are planning to migrate to BTRS, multiple other PHJs are in the process of procuring BTRS, and many more are requesting proposals for BTRS. To the best of our knowledge, there is no other vendor with more than one client for meeting all of the Focus Area E HAN requirements. Also, there is no other vendor that has their technology proven in full production anywhere near the extent that Virtual Alert can demonstrate.

Virtual Alert team is already developing the next product lines, which will meet other public health information requirements in a way that seamlessly integrates with HAN. One example of this is the newly available PVMS module (Prophylaxis and Vaccination Management System). Products like these prove Virtual Alert's commitment to continuing innovation in public health information systems, as well as BTRS's ability to serve as a core communications and information exchange platform—it is a complete HAN, but is far more than just a HAN.

Virtual Alert has already developed multiple strategic partnerships to develop, market and deploy its products. These include multiple divisions within Microsoft (covering all three of the aforementioned partnership aspects) and HP/Compaq. Virtual Alert is Microsoft's top Health & Human Services partner for bioterrorism solutions and one of three partners being featured nationally by the Homeland Security solutions team.



Additionally, multiple integrator companies are forming and proposing partnerships with Virtual Alert, as they are seeing our clear leadership in this space. Virtual Alert is a privately owned company, funded by the management team and by private investors. It has a self-funding, and hasn't applied for venture capital nor does it intend to do so. Virtual Alert, Inc. is incorporated in California. We maintain offices in Sacramento, California, La Jolla, California, and Austin, Texas.



APPENDIX 2 (b)
SUBCONTRACTED SERVICES – EQUIPMENT, LOCATION,
AND SERVICES



Michigan Health Alert Network Subcontracted Services Equipment Location and Services

Virtual Alert will provide the equipment location and hosting services for the primary and backup sites for the Michigan Health Alert Network through SureWest of Sacramento, CA and Inflow of Austin, TX, respectively. They are addressed in turn.

1. Firm Name of the subcontractor(s)

Surewest

2. Address

SureWest Communications
P.O. Box 969
Roseville, CA 95678

3. Contact Person

Richard P. Starr
SureWest Broadband, Major Accounts Manager
Phone: 916-746-3078
Mobile: 916-768-1899
Fax: 916-780-8797
E-mail: r.starr@surewest.com

4. Complete description of work to be subcontracted

This subcontractor is responsible for providing the physical space where the primary production system will be placed. SureWest will provide a highly secure and disaster-proof space for the MDCH system. They will also enforce strictly controlled access to the physical system. SureWest will be the subcontract ISP provider. SureWest will be responsible for the availability and performance of the ISP service, providing backups should the primary Internet connection fail. Similarly, SureWest will be providing the telephonic service for telephonic alerts, fax alerts and fax distribution of documents from the portal.

5. Descriptive information concerning subcontractor's organizational abilities.



Building 20, McClellan Park

~Brief History~



Building 20 was originally built in 1938 as the base infirmary and later converted to the base communications building. The building is a cast in place concrete structure with a built-up roof. The building was originally fed from a 400-amp service that passed through Building 14 from the north. The north half of the building was primarily office and break-room space, while the south half housed the communication switch room and miscellaneous equipment. The facility was well worn and dated.

~Major Improvements~

- New 15-year single-ply roof.
- Exterior infrastructure for SMUD to not only serve Building 20, but to service adjacent buildings will allow for a future tie to loop feed on the east side of the building. This will allow SMUD the ability to feed the building from two different directions thus increasing redundancy at the site.
- Computer Room has two 20-ton CRAC cooling units, which are sized to give redundancy to the computer room. Standard rooftop mounted units serve the offices.
- Fire Suppression System, designed and installed by Sabah International, is a technologically advanced FM 200 pressurized gas system. FM 200 will suppress any fires without causing damage to the electronic equipment.
- State-of-the-art C-Cure card reader access system with 24/7 camera surveillance.
- New exterior insulated windows.
- 1,800 square feet of computer raised access flooring.

~Electrical Features~

Service: 2000 amp 480/277 Volt with 100% Generator Backup by IEM.

The following is included within the main pad mounted equipment enclosure:

- 2000 Amp 480/277 volt meter and main breaker section.
- 2000 Amp 480/277 volt automatic transfer switch with maintenance bypass switch.
- 2000 Amp 480/277 volt metering section.
- 2000 Amp 480/277 volt distribution section
- 750 KVA 480 to 208/120 volt transformer.
- 2000 amp 208/120 volt meter section
- 2000 amp 208/120 volt distribution section.

Generator: 1500 KW 480/277 volt by Onan/Cummins

With the following:

- 2000A 100% rated Main Breaker
- Sound Rated Enclosure with Diesel Fuel Tank
- Alarms are remotely monitored

2000 AMP Manual Transfer Switch for Portable Generator by IEM



With the following:

- 2000 amp 480/277 volt 100% rated switching between Main generator and Temporary Generator.
- Connection points for 1500 KW Portable Generator
- Control switching and auxiliary power connections are also included.

300 KVA UPS System 480 volt input/output by Liebert

With the following features:

- At this time 180 watts of UPS power per square foot are available to the raised floor area.
- 27 minutes of battery backup at full load Monitored alarms
- Power Conditioning is provided by various means.
- A dual output Harmonic Mitigating Transformer is used to convert the 480-volt output of the UPS to 208/120 volts.
- Clean Power is delivered through a Split Distribution System.
- This system can be operated from the main 208/120 volt distribution switchboard should there be a catastrophic failure of the UPS System.

Reference:

County Medical Services Program (CMSP). The contact there is Lee Kemper, 916-554-6424.

1. Firm Name of the subcontractor(s)

Inflow, Inc.

2. Address

Inflow, Inc.
8025 IH 35 North
Austin, TX 78753

3. Contact Person

Scott Rayer, Sr. Regional Business Development Manager
(512) 531-5432
(512) 426-9702 (Cell)
srayer@inflow.com

4. Complete description of work to be subcontracted



This subcontractor is responsible for providing the physical space where the redundant system will be placed. InFlow will provide a highly secure and disaster-proof space for the MDCH system. They will also enforce strictly controlled access to the physical system. InFlow will be the subcontract ISP provider. InFlow will be responsible for the availability and performance of the ISP service, providing backups should the primary Internet connection fail. Similarly, InFlow will be proving the telephonic service for telephonic alerts; fax alerts and fax distribution of documents from the portal.

5. Descriptive information concerning subcontractor's organizational abilities.

See rest of section.



Inflow Services Overview

Inflow, Inc.

Scott Rayer
Sr. Regional Business Development Manager
8025 IH 35 North
Austin, TX 78753
(512) 531-5432
(512) 426-9702 (Cell)
srayer@inflow.com
www.inflow.com

*Inflow's mission is to provide our Customers with the most reliable,
Secure, seamless, and proactive outsourced IT services in the world.*

We will continuously define the quality standard in our industry.



I. Table of Contents

I. Table of Contents 57

II. Why Inflow? 58

 COMPANY INTRODUCTION AND STRATEGY OVERVIEW 58

 PRODUCTS AND SERVICES 59

 MARKET DIFFERENTIATION..... 69

 SOLUTION 72

This document is intended solely for the internal use of prospective customers to evaluate the possibility of a business relationship with Inflow. The information provided in this document is protected by copyright and shall not be copied, distributed or otherwise shared with any other company or used for anything other than the intended use. Much of this information is proprietary to Inflow. This document is not intended to be a binding contract or document. The relationship between Inflow and the company requesting this response is not binding until Inflow's Internet Data Center agreement is executed by both parties.



II. Why Inflow?

In the section below, Inflow has provided a response to this question by briefly discussing Inflow's history, plan, products and services, and market differentiation. In some cases these responses are short and more specific information about Inflow and its products and services is available from your sales executive. Finally, a solution is proposed that includes a network diagram and pricing for the components required for your solution.

Company Introduction and Strategy Overview Background

Inflow was founded in 1997 and is headquartered in Denver, CO. Currently, Inflow manages 13 data centers in Tier 2 markets across the United States. Inflow's mission is to be the service quality leader in outsourced IT services for enterprises with mission critical applications.

Inflow's original service model was basic collocation and network management services. Over the past five years, Inflow's model has evolved to include a number of high quality managed services supporting three primary lines of business: Application Hosting and Management, Business Continuance Services, and Enterprise Data Center Management. Today our

comprehensive list of products and services are hardware and software agnostic and our IDCs are carrier neutral providing maximum flexibility in supporting our customer's requirements whatever they are.

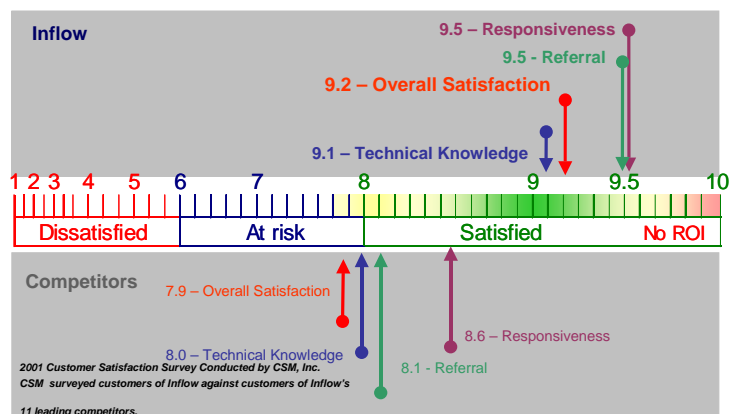
Today, Inflow supports over 750 customers across IDC locations and has consistently achieved industry leading customer satisfaction scores conducted by an independent third party. Key in the realization of these accomplishments is Inflow's business model that provides local operations support in each IDC. Additionally, each customer is assigned a dedicated operations technician to work with for the life of the business arrangement with Inflow. This individual is backed by an entire team of highly trained employees, documented processes and procedures and our proprietary operations support system (OSS) called FlowTrack. Flowtrack automates routine tasks and ensures consistency in issue tracking and communications with our customers.

Some of the companies that Inflow provides services to with business models similar to many prospective customers are ecommerce companies like the following: eBags, MapQuest, Hoovers Online, law.com, randmcnally.com, netLibrary, hire.com, akamai.com, Webex, and Dataplay.

Providing outsourced IT services is Inflow's core business – it's the only thing we do. Inflow takes service delivery seriously and works very hard to make sure our customers are happy.



Service Excellence Differentiator



Customer Survey, 2001, CSM, Inc.



Recent Accomplishments

- Achieved industry leading 4th quarter 2001 financial results. Revenue and total customers increased 7% over the previous quarter.
- Awarded Colorado's "Fastest Growing Private Company" by The Denver Business Journal – April 2002
- Selected as an exclusive member of IBM 's Hosting Advantage Program. Inflow and IBM will partner to provide fully integrated solutions for enterprise customers.
- Received industry-leading rating of 9.2 on a 10-point scale for overall customer satisfaction, exceeding the industry average score of 7.9. The survey was conducted by Atlanta-based CSM, a leading customer satisfaction consulting company.

Products and Services Overview

Inflow 's premier products and services are organized into four functional lines of business:

- Professional Services
- Managed Application and Infrastructure Services
- Performance Optimization Services
- Managed Network and Hosting Services

Inflow integrates and delivers these services through three primary practices:

- Application Hosting and Management
- Business Continuity and Disaster Recovery
- Enterprise Datacenter Management (EDM)

Products and Services

State-of-the-Art Internet Data Centers

Inflow constructs data center facilities with redundancy and security as paramount considerations. This foundation helps to ensure that the architecture customers deploy will have maximum availability and reliability for their end users. Inflow uses standardized equipment to ensure consistency in support no matter which data center(s) you have equipment in.

Redundant Power Supply System

Redundant power protects your mission-critical application against service interruptions. Inflow's unique hot sync parallel/redundant systems provide redundant power supply through Uninterruptible Power Systems (UPS) and backup generators to guarantee no interruptions in service.

High Security Facility (Inside and Out)

Inflow stores names (on an authorized access list) in a proprietary secure database. When you or someone on the authorized list comes to the facility, Inflow requests to see photo identification. If the name and photo on the I.D. matches the name and photo in our secure database, entrance is granted. Once inside the facility, Closed Circuit Television (CCTV) cameras mounted above each cabinet row monitor all activity. There are card readers on every door within the facility, and unique card readers on the doors to the suites. Only Inflow is allowed to open and lock equipment cabinets. Additionally, there are no customer names on the cabinets and no cabinet floor plans to associate cabinets with customers.

Customized Cabinet Sizes

Inflow offers a selection of lockable cabinet sizes to house your application. Inflow's standard cabinets are 84 inches high, 19 inches wide and 36 inches deep. Inflow will install and connect your customer equipment to building ground, electrical power circuits and telephony cabling. The cabinets can be connected to multiple communications carriers for optimal performance and redundancy. Inflow also offers secure suites as an option for customers with additional security requirements or for those with equipment that cannot be secured in standard cabinet enclosures.



Multi-homed and Carrier Neutral Solutions

Inflow provides carrier neutral solutions for your leased line, ATM (asynchronous transfer mode), ISDN (integrated services digital network) and data network circuits. Multiple Tier 1 carrier options ensure the most cost-effective solutions. We can architect a solution for complete redundancy and maximum performance. Inflow will back it all with a guarantee of 100% availability.

High Capacity Heating, Ventilation & Air Conditioning (HVAC) System

Your equipment is monitored in a temperature-controlled environment. Inflow's Internet Data Centers operate at an average temperature between 65 and 75 degrees Fahrenheit and average relative humidity between 30 and 45 percent.

Fire Detection & Suppression System

Inflow's Very Early Smoke Detection Apparatus (VESDA) system detects abnormal particulate matter in the air. A pre-activation fire detection system verifies a fire before activating the suppression system. Heat detectors above and below both the floor and ceiling are monitored and controlled in the NOC (Network Operations Center) and also monitored offsite.

Raised Floors for Organized Cabling



Raised floors enable Inflow to place power and cabling below the floor of the facility for optimal security. All power and CAT 5 data cabling is placed sub-floor in a horseshoe fashion (to eliminate interference between power and data cables). The raised floors and zoned cabling are designed to support 1250 lbs. point load.

Local and Long Haul Circuits

Local loop connections are provided by a variety of (LECs). Each Inflow IDC has local fiber connectivity from 2-4 LECs and relationships with multiple providers of long haul circuits. Customers also have the option of purchasing circuits directly from any network provider. Inflow will provide Carrier Facility Assignments (CFA) for a small monthly cross-connect fee if this option is preferable. Inflow monitors all network circuits and will proactively monitor, troubleshoot, and escalate to network providers for trouble identification and resolution in the event of trouble.

InflowNet - Internet Access

InflowNet is a multi-homed, managed Internet access service that provides the ultimate in availability, performance, and scalability. InflowNet connects you directly to multiple backbone Internet Service Providers through private transit connections. InflowNet 3.0 delivers up to 4 Gigabits per second of total Internet throughput per Inflow facility and provides you with optional Gigabit Ethernet connections.



Inflow purchases private transit from Tier 1 ISP providers (2-5 providers per IDC) that guarantees network availability, scalability, and performance. In our transit arrangements, instead of becoming a peer of another network, Inflow pays other infrastructure providers for interconnection privileges that fully extend to the transit provider's peers. In this case, the buyer (Inflow) of the transit services becomes a customer of the provider.

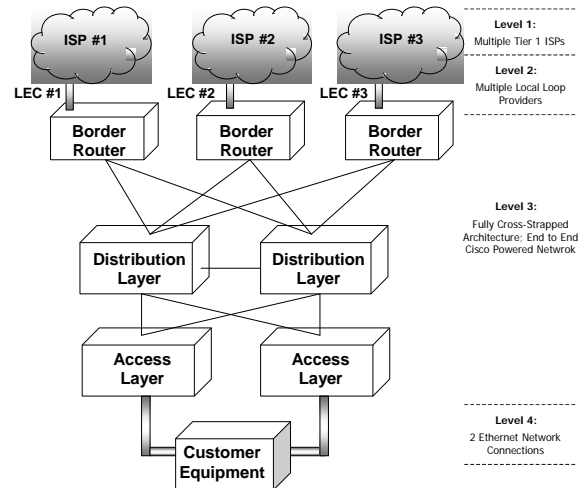
Our private transit arrangements have direct network connections to the transit provider's equipment. Because these connections to transit provider's networks are direct, data quality and throughput are high. In this arrangement, the transit provider will route its transit customer's traffic over the networks of its peers as well as over its own network.

The Value of InflowNet:

Availability: 4 Layers of Redundancy

InflowNet was designed from the ground up with the primary goal of providing 100% availability of the Internet to your equipment. This goal is obtained through multi-homing, BGP-4 and 4 layers of redundancy:

- Layer 1 – Multiple Tier-1 ISPs
- Layer 2 – Diverse local loop providers connect InflowNet to each ISP
- Layer 3 – Fully Redundant Cisco Powered Network (a.k.a. InflowNet Mesh)
- Layer 4 – Use of HSRP (Hot Standby Routing Protocol) to provide physically redundant Fast Ethernet or Gigabit Ethernet connections from separate access layer switches to your equipment cabinet.



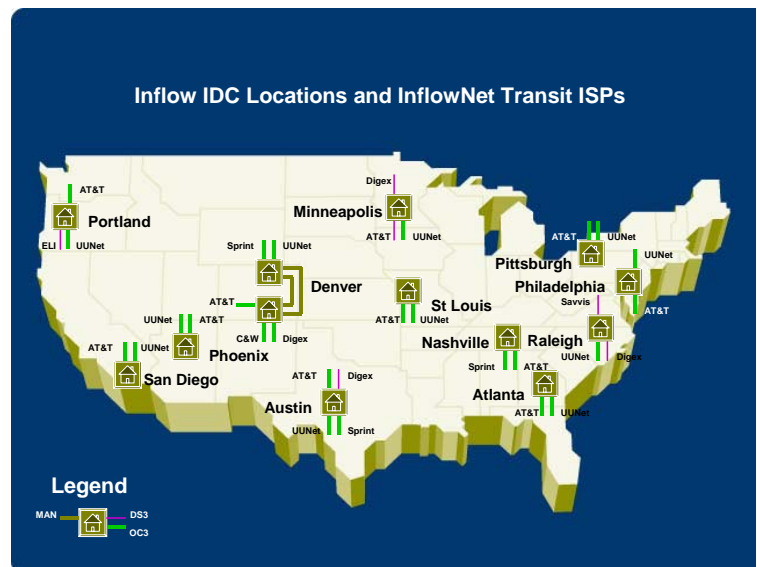
Local loop connections are provided by a variety of Local Exchange Carriers (LECs). Each Inflow Internet Data Center has local connectivity from 2 to 4 LECs. InflowNet utilizes two or more of these LECs in each Inflow Internet Data Center, ensuring the local loop is not a single point of failure.

Performance: Transit Connections

InflowNet maintains direct transit connections to the backbones of end-users. Inflow's ISP partners connect approximately 60-80% of Internet end-users directly to their backbones. By connecting the Inflow Internet Data Center and your application directly to these backbones, InflowNet reduces the distance between your end-users and your application. In addition, these direct connections reduce the reliance on congested public and private peering points because traffic is put directly on the destination backbone.

The effect is increased performance for your customers. However, at times it is still necessary to exchange data with smaller ISPs. Inflow's Tier-1 ISPs have over 300 combined private peering relationships. Private peering ensures increased performance and reduced packet loss over public peering.

Scalability: Bandwidth Utilization





Through the use of multiple ISPs, Inflow has bi-directional bandwidth scalability. Based on your need, Inflow may choose to scale bandwidth with an existing ISP (Vertical Scalability) or may choose to add a new ISP to the mix (Horizontal Scalability).

Inflow IP Engineers closely monitor the utilization of Inflow's available bandwidth capacity at each of its IDCs to ensure that we always have an acceptable amount of capacity available for customer growth. Unlike other providers that may oversubscribe their bandwidth capacity, Inflow proactively upgrades its capacity before critical thresholds are reached.

Network/Internet Connectivity Design

The network component consists of the local loop circuits and the paid transit connections to Internet Service Providers. Multiple Tier 1 Internet Service Providers (ISPs) are connected to each Inflow Internet Data Center.

Dedicated Bandwidth vs. Shared Bandwidth

Inflow offers dedicated bandwidth; we manage network capacity so you do not compete for bandwidth with other Inflow customers.

The InflowNet Mesh

InflowNet 3.0 runs on a completely redundant, end-to-end Cisco Powered Network utilizing Cisco 7206 VXR and 12008 GSR Border Routers with Cisco 6509 Catalyst Switches in the Distribution and Access Layers. You are assigned to a unique Virtual Local Area Network (VLAN). Dual 100mb Ethernet or Gigabit Ethernet connections are provisioned directly to your equipment cabinet. You can either be routed or switched directly to the access layer based on your needs. Enhanced Interior Gateway Routing Protocol (EIGRP) and Hot Standby Routing Protocol (HSRP) are enabled, providing seamless connectivity in a fail-over situation.

InflowNet IR (Intelligent Routing)

Inflow has developed a proprietary Intelligent Routing (IR) solution that optimizes the core components of the InflowNet product. Inflow's IR works in the following way: The customer's web site has an HTML string that causes the web site visitor to identify himself to Inflow's IR system. Upon identification of an end user (source IP address) the border routers are each sampled to determine the quickest path. The mesh is updated to direct all outbound traffic through the selected router for that specific web site visitor.

Inflow's IR system utilizes an Internet performance-based methodology to dynamically select the best path directly to your end user. This methodology can automatically adapt routing to avoid common problems in the Internet such as fiber cuts, congestion, routing black holes, and misconfigured routing equipment.

Keynote and Inflow accomplished four weeks of testing using sites in Production during June and July of 2001:

- IR provided a 14% average improvement in downloads where web sites weren't the bottleneck
- IR improved BGP route selection at least 45%
- Performance was improved significantly for poor performers—poor performers in test saw 20%-30% improvement
- Can route around Internet problems by design including Black Holes, BGP convergence, and Network Congestion
- According to Keynote, final test results understate IR's effect on performance and Internet availability

EvenFlow - Local Web Server Load Balancing

EvenFlow Local, Web Server Load Balancing, is a managed service that helps customers improve web site availability and responsiveness by directing traffic to the best-performing web server within an Inflow IDC. In the case of a server failure, EvenFlow Local automatically redirects traffic away from the failed server. EvenFlow's architecture, utilizing redundantly configured Alteon load balancing switches, ensures continuous availability of the load balancing solution. Inflow will manage all aspects of the configuration,



maintenance and troubleshooting, as well as session-state maintenance for client-server connections. The customer will be responsible for making any changes to customer-owned equipment or applications.

Akamai – Content Delivery Services

Inflow offers a full set of Content Delivery and Load Balancing Services through our relationship with Akamai Technologies. Akamai services are complementary additions to our top of the line InflowNet Internet Access offerings. Combining InflowNet with Akamai Content Delivery Services will deliver maximum performance and optimal end user experience to web sites. The Akamai services that Inflow offers fall into 4 categories:

- Static Content Delivery (Caching) Service – Akamai FreeFlow
- Live and On-Demand Streaming Media Services – Akamai FreeFlow Streaming
- Entire Web Site Delivery from the Network Edge – Akamai EdgeSuite Service
- Global Server Load Balancing (GSLB) Service – Akamai FirstPoint and FirstPoint Failover

Inflow offers customers seamless implementation, Tier 1 support and billing for Akamai services, providing customers with the same top quality customer service that they receive for all of Inflow’s other product offerings.

Inflow Managed Security Services (MSS)

Inflow employs MSS staff that operates our Security Operations Center (SOC) 24x7 to support a complete line of security products including over 200 firewalls and other security devices for our customers today. Technology vendors including CheckPoint, Cisco, and the Global Incident Analysis Center (GIAC) certify Inflow engineers.

Inflow’s managed firewall service stands as the first line of defense in safeguarding the network against unauthorized access. Inflow offers both single and high availability solutions on multiple hardware platforms and can provide customized and professional support guidelines and tools to make sure you have the best security policy in place based on your security needs.

Other services offered as part of Inflow's MSS suite of products include:

- Emergency Response Services
- Managed Intrusion Detection Service
- Managed Network Services
- Managed VPN Services
- Remote Scanning Services

StorageFlow – Primary Storage Service

Delivered as a disk storage utility, StorageFlow provides secure, virtually unlimited access to a shared disk infrastructure to customers collocating with Inflow’s Internet Data Centers. The fibre-channel attached and RAID protected storage can be requested and implemented on a “pay as you grow” basis.

StorageFlow allows you to concentrate on your business rather than worry about capacity planning, operating expenses or retaining skilled storage professionals. Inflow assumes responsibility for the design, implementation and operation of StorageFlow. This storage solution includes the necessary network infrastructure, storage equipment, software and operations (management, maintenance and support) needed to meet your changing business requirements.

StorageFlow Gold	Benefits
<ul style="list-style-type: none"> • Host connectivity: Dual fibre channel connection with support for load-balancing and automatic failover. Multiple network paths between the fibre-channel fabric and the storage array offer additional levels of redundancy. • Data protection mechanism: Integrated array based data protection 	<ul style="list-style-type: none"> • StorageFlow Gold provides you with the most highly available and highest performing, fault tolerant storage service available in the market today. • With support for options data replication and mirroring capabilities, StorageFlow Gold provides you with the utmost of expandability.



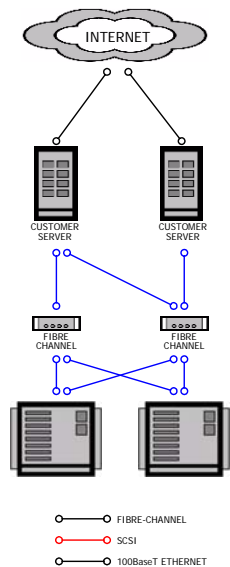
<ul style="list-style-type: none"> Operating system support: Tier 1 and Tier 2 servers (Tru64, AIX, HPUX) as well as support for boot devices and standard clustering technology. Capacity buffer: The StorageFlow service includes a 10% buffer in the event the contracted amount is consumed. Storage expansion: Up to 200Gbytes can be added within 24 hours. Migration services to Gold Service Level Administration: 24x7 GridWatch™ monitoring. 	
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

Security

All StorageFlow Primary Data Storage services are provisioned using a fibre-channel based storage area network. To ensure your data is not compromised, Inflow utilizes both LUN masking and zoning as key enabling features. Additionally, each port on the fibre channel switch is assigned to a specific customer zone to ensure that no rogue clients have access to any disk array. Access to the disk arrays, servers and network switches is restricted to authorized personnel.

Technical Description

StorageFlow features a storage area networking (SAN) architecture for superior performance, security and data availability. This SAN architecture is based on an end-to-end Fibre channel infrastructure featuring the latest in SAN fabric switching technology. Using SAN, you can connect to the Inflow fabric and, based on security configuration parameters share a wide range of storage services.



StorageFlow – Tape Backup and Restore Services

The ultimate data protection against data corruption and accidental loss is provided by regular, managed tape backup. Inflow's StorageFlow – Tape Backup and Restore Service provides an enterprise-class tape backup solution.

The Tape Backup and Restore service is a fully managed and monitored service designed to ensure data restorability in the event of disk crashes, application and user errors, viruses and web site sabotage that can take businesses permanently off-line. Intentional or not, these problems can be severe enough to lose customers, hurt investors' confidence, and impede revenue. Yet, some companies gamble on not having backup and restore solutions adequate to get them back in business.

StorageFlow Tape Backup and Restore	Benefits
<ul style="list-style-type: none"> Backup Schedules: 6 incremental backups performed daily and one full backup performed weekly. Retention: All backups are retained for 14 days from the time of creation. Restoration: Customer initiated restores occur within 60 minutes of request. Up to 5 restores can be requested in a given month without additional cost. Reporting: monthly reports include consumption and performance related information. Administration: 24x7 monitoring and hands on administration. 	<ul style="list-style-type: none"> The StorageFlow Tape Backup and Restore service provides you with piece of mind. By knowing your data is safe and always available for restore your application and operations people can feel more comfortable performing their daily administrative tasks and not be burdened by daily backup tasks.



Security

To ensure security and to provide the best possible performance, data backup is performed over a second private network that does not have any connectivity to the Internet. Security is enhanced through the use of a switched Virtual LAN (VLAN) architecture. This switch ensures one customer cannot “see” another customer’s data.

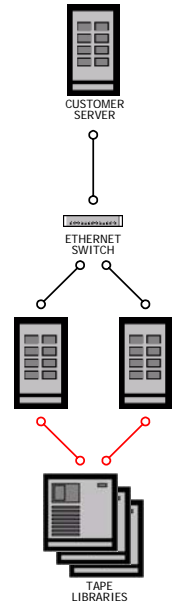
All on-line data residing within the libraries is accessible only by designated users from whom it originated or other administrative personnel previously approved by you. This level of security is administratively controlled through the backup master server. Access to the libraries is restricted to authorized personnel. When tape cartridges are removed from the tape library, they are separated and securely handled at all times.

Technical Description

Copying all of the critical data to tape once a week (full backup), and copying all data that has changed since the full backup on the other days of the week (incremental backup) protects data. This cycle is repeated weekly. Data is maintained on tape long enough so that at any time data up to two weeks old can be recovered.

Backup software is installed on each of the servers to be backed up. This software communicates with the backup server software to manage the selection of files and schedule the backups. When databases are involved, additional software must be installed and configured.

The infrastructure Inflow provides is comprised of redundant backup servers, a high performance tape library and tape drives. The backup servers manage the backup schedules and restore requests for the entire Internet Data Center. They also manage all of the your core business and forego the daily tasks associated with data protection.



AIMS - Deep Monitoring of Customer Hardware and Software Systems

(i) Monitoring & (ii) Alarms/response

Inflow's Premium Application and Infrastructure Management Services (AIMS)

Inflow 's Premium Application and Infrastructure Management Services (AIMS) are designed to support mission-critical e-business environments. Our advanced monitoring technologies and comprehensive response processes provide end-to-end, 24x7 monitoring and management of the entire technology stack, including network devices, web servers, operating systems, databases and applications.

Supported Platforms

Hardware	Operating Systems	Databases	Applications
Cisco	UNIX	Oracle 7,8,8i	E-Commerce
F5	Sun Solaris	Microsoft	ATG Dynamo
Nokia	IBM AIX	MS SQL Server 7	WebLogic
Alteon	HP-UX	SQL 2000	Oracle e-Bus 11i
3COM	LINUX		
Nortel	Microsoft		Oracle Financials
HP	NT 4.0		Web Servers
Dell	2000 Adv. Server		iPlanet
Compaq			IIS, SiteServer
Sun			Apache

Levels of Service

Level 1 - Monitoring and Notification

- 24x7 Monitoring, Alert Validation and Notification
- Synthetic Transactions



- Dedicated Web Portal
- Real-Time Custom Reporting

Level 2 - Proactive Maintenance

Level 1 Services Plus:

- Incident Resolution
- Basic Troubleshooting
- Scheduled Proactive Services
-

Level 3 - Total Management

Level 1 & 2 Services Plus:

- Problem Management
- Root Cause Analysis
- Patch Management
- Performance Tuning
- Backup and Recovery Management

Level 4 - Consulting

- Network and Application Design and Consulting
- Change Management
- Version Upgrades and Installs
- Site Transitioning
- Stand-By Local Engineering Support

(iii) Reporting

FlowView™ (Inflow Customer Portal)

Premium AIMS information is viewable through Inflow's secure, web-based FlowView Customer Portal. Here, customers can view critical information such as:

- Contacts, Roles, Escalation Rules, Assets and Managed Service Agreements
- Event Control: Interactive Event Management and Status
- Trouble Ticket History

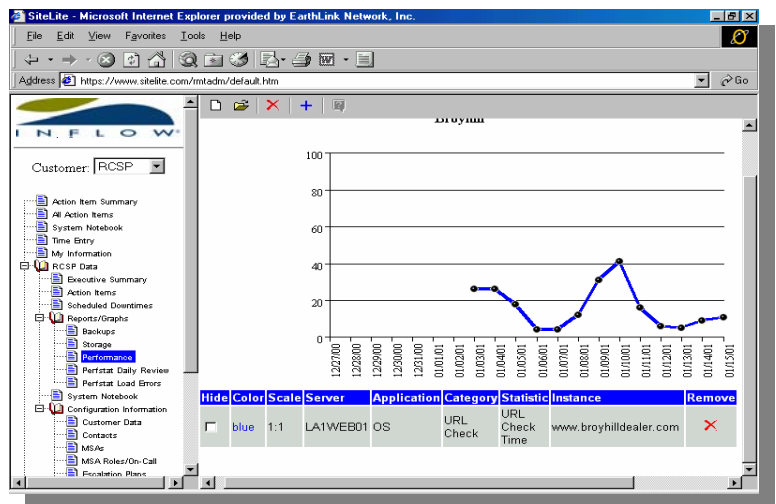
(iv) Backups/Fault Tolerance

There are multiple redundancies built into the solution framework so the customer's applications and infrastructure are being monitored 24 hours a day. This can only occur with redundant and self-sufficient NOC's and architecture. Monitoring is executed at the local Inflow data center as well as NOC's in Dublin and Irvine, CA.

FlowView - Customer Access Portal

FlowView™ is Inflow's 24x7 Web portal that provides you access to near-real-time information about your collocation services. Simply log on to www.inflow.net to view information as it exists in Inflow's secure internal databases, including:

- Bandwidth Statistics
- Current Latency (on the InflowNet Network by IDC)
- Current Bandwidth Usage
- Invoices
- Security Lists
- Authorized Access List
- Monthly Access List
- Troubleshooting Information





- Network Diagrams
- Work Orders
- Trouble Tickets

In addition, you only have to log on once to view information for all of your locations. FlowView is accessible from Internet Explorer (version 4.0 or higher) or Netscape (version 4.0 or higher.) Secure access is provided through a secure server using SSL (Secure Sockets Layer) 128-bit encryption and confidential user names and passwords protect all of your information.

Tiered Operations Support - Onsite 24x7

Dedicated Relationship Management

An Inflow Project Manager will be assigned to your account from our Strategic Project Management Team. Your project manager will actively track and manage all aspects of the implementation process for you. They are also available to manage details on your side of the implementation at your request. Additionally, a single point of contact will be assigned to your account that is a member of the operations team at the IDC and will ultimately become the owner of the technical relationship with your account. Finally, your sales account manager will continue to maintain a relationship to support the appropriate development and the continuation of a strategic and formal business relationship. Those people are:

Bob Brown
Strategic Project Manager
Rbrown@inflow.com
512-531-5400

Operations Technician – Will be assigned prior to installation.

Scott Rayer
Senior Account Manager
Srayer@inflow.com
512-531-5432

Tiered Technician Support

Inflow provides Tier-1 technician support for basic tasks such as system backups, media replacement, reboot, and on-site "hands" for your specialists. The following information outlines Inflow's tiered technical support services and the costs associated with each.

Inflow Tier 1 Support

Cost: Free of charge

Includes:

- Rebooting of equipment (servers, PCs, routers, etc.)
- Phone support with basic command line instructions (less than 30 minutes)
- Cable management or testing/troubleshooting
- Inflow-ordered circuits: network troubleshooting/testing (loop backs, stress tests, etc.)
- Customer-ordered circuits: Up to 30 minutes of network troubleshooting/testing

Inflow Tier 2 Support

Cost: \$100/hour

Includes:

- Greater than 30 minutes of phone support with basic command line instructions
- Vendor troubleshooting
- Equipment installation
- Customer-ordered circuits: Greater than 30 minutes of network troubleshooting/testing



Inflow Tier 3 Support

Cost: \$200/hr. for scheduled support services - \$250/hr. for unscheduled support services between the hours of 11 p.m. and 6 a.m.

Includes:

- Router configurations and maintenance
- Sniffer/protocol analysis
- Hardware/software support (swapping of cards, installation of system software, etc.)
- Network/IP consulting
- Network design
- Security/Firewall reviews
- IP management

Proven Operational Systems and Process

FlowTrack

FlowTrack is Inflow's proprietary software application engineered to integrate and automate business processes. This scalable application allows Inflow to quickly implement network and equipment provisioning through electronic work orders issued to operations technicians in each facility. FlowTrack is a critical component of Inflow's 30-day up-and-running guarantee. It allows Inflow to rapidly and efficiently scale network management across a broad network of Inflow facilities to meet the needs of growing e-businesses. FlowTrack integrates multiple modules, each focusing on a different aspect of management—asset management, network operations, account billing management, and customer care.

Inflow Escalation Procedures

In the rare instance of anything going awry with your Inflow product/service, Inflow begins by following the general customer troubleshooting procedure. Once the root cause is identified, Inflow will document all actions taken and issue a trouble ticket using our automated system, FlowTrack. Inflow prides itself on developing a close relationship with all customers. If anything would go wrong, with any type of network/security issue – we will call you, right away, and keep you informed as to the progress of our troubleshooting.

Trouble Tickets

Trouble Tickets at Inflow differentiate us from our competitors. We want to provide information in three sections: Problem Description, Troubleshooting, and Corrective Action. Corrective Action is extremely important because we want to show that although everyone makes mistakes -- Inflow communicates mistakes whether they are vendor, customer, or internally produced so everyone can learn from their mistakes and prevent them in the future.

Inflow Customer Life Cycle Process

All Inflow customers deserve the same world-class customer service, from initial contact through ongoing account management. The Customer Life Cycle defines a standard structure for sales, implementation and management of all accounts by defining deliverables and accountabilities required to seamlessly implement your solution. Three major processes define the Customer Life Cycle: the Prospect to Customer Process, the Customer Implementation Process and the Account Management Process.

The Prospect to Customer Process

This process matches your needs to Inflow's service offerings. Key deliverables of the process include a Non-Disclosure Agreement, Credit Application, Contract Terms and Conditions and clear requirements.



The Customer Implementation Process

This process was defined for the following needs:

- Making the Sales to Operations hand-off seamless
- Preparing for the installation through a pre-implementation meeting
- Meeting to review the requirements in an implementation meeting
- Completing the technical details in the Customer Design Requirement forms
- Defining detail in the Customer Notebook

Inflow establishes a Customer Notebook for each customer. Some of the major elements in the Customer Notebook include the network diagram, single points of failure analysis and specific troubleshooting procedures that match your architecture. All of the gathered information is available in hard copy at the IDC and via the FlowView customer portal.

Documented Application Design and Support Procedures

Part of every solution Inflow delivers to customers and partners includes documented process and procedure to ensure consistency in delivering the best solutions to our customers. Below is a logical view an example design representative of a typical production site. This logical diagram along with other critical information about the solution will be captured during the installation process by technicians and engineers working on the solution. As information is gathered it will be added to the customer notebook and posted to the FlowView customer portal. Scheduled future communication times will ensure constant improvements and ongoing accuracy of the information about the customer environment.

Market Differentiation Service Philosophy

Inflow's philosophy for providing high quality IT services is tied to 3 core elements:

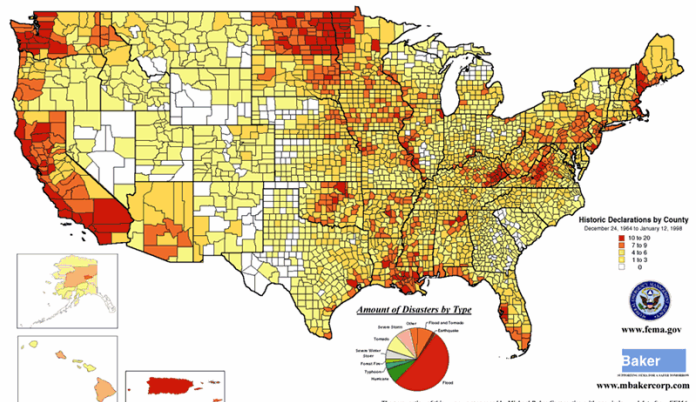
1. Hiring Good People – Inflow directly hires and trains all on site operations personnel and requires certification in various areas of technical expertise. Inflow believes that by having highly trained people locally interfacing with our clients, we can provide a better quality of service.
2. Process – Inflow is currently pursuing ISO 9000 certification and we currently have documented over 400 critical business processes. By documenting good process, Inflow has the ability to scale quickly as well as provide consistent high quality of service across all data centers.
3. Systems – Inflow relies on a proprietary OSS called Flowtrack to integrate all departments within the company. The outcome is the ability to provide a higher level of service to our clients because every department within Inflow is referencing the same information and workflow is automated. Items such as work orders, trouble tickets, and routine maintenance are all automated in Flowtrack improving operations efficiency and reducing the potential for human error.

Tier 2 Market Presence

Inflow operates exclusively in Tier 2 markets. In other words, Inflow has IDCs in cities like Denver, Minneapolis, and Raleigh rather than locations like Chicago, New York City, and San Francisco. From a disaster recovery/business continuance perspective most Inflow locations are considered to be at lower risk of outage due to both natural disasters and terrorist attacks.

Critical System and Process Redundancy

HISTORICAL PRESIDENTIAL DISASTER DECLARATIONS 1,198 DECLARATIONS SINCE 1964



"To successfully mitigate against disaster will require the combined talents and concerted efforts of all levels of government, academia, professional and voluntary organizations, the corporate sector, and all Americans."
- Bill Clinton, December 6, 1995



Any Inflow data center can fail over monitoring capabilities to any other data center providing our clients with maximum redundancy. Because customer custom troubleshooting and escalation procedures are maintained digitally, even in the event of a failover to a remote NOC, Inflow will be able to continue to monitor and support your mission critical applications.

Dedicated Account Management

Inflow will provide each customer with a dedicated account team including a dedicated operations technician for the life of the business relationship. Inflow allows each client to create customized troubleshooting and escalation procedures so that we can support each customer with maximum effectiveness. These procedures are maintained in both hard copy at the data center and digitally in our proprietary system. While our customers have dedicated resources to work with, Inflow never creates a single point of failure – all of our people are empowered to help.

Strongest SLAs in the Industry

Inflow provides strong individual Service Level Agreements for every service we provide. For example, Inflow provides 100% availability on our Internet service (Inflownet) as well as a 100% Power Availability SLA within the data center. This fact is indicative of our own confidence in our products and services and gives you the personal assurance that our products are not one-off solutions but rather fully tested and supported enterprise solutions.

Customized and Flexible Solutions

One of Inflow's strongest value propositions is its ability to accommodate the changing needs of our customers quickly and efficiently. Although Inflow is a national provider, service delivery and support are driven at the local data center. Because Inflow will assign each customer with a dedicated operations point of contact, the local operations team can handle any changes to services immediately. This includes service additions – many of which can be processed within 24 hours (once paperwork is executed). Rapid deployment of services includes, but is not limited to, increases in bandwidth, additional cabinet space, additional power circuits, and basic monitoring. Additionally, all Inflow services carry an Installation Service Level Agreements on each service providing added incentive for quick installation. In short, Inflow offers a wide variety of services from basic collocation to 24x7 monitoring and management of proprietary applications – we can accommodate the changing needs of evolving companies.

Carrier Neutral

Inflow's IDCs are carrier neutral and our support for solutions is technology agnostic. This gives our customers maximum flexibility in building solutions that Inflow can support.

Financial Stability

Inflow is a strong national provider of outsourced IT services. Inflow is EBITDA positive as a company and expects to be cash flow positive by the end of 2002. There are several factors that contribute to Inflow's success including Inflow's unique operating model: tier 2 markets where Inflow has had first mover advantage, smaller data center size (no larger than 20,000 Sq. Ft.), and other differentiators mentioned in this section.

Given the financial stability of Inflow and the fact that outsourcing is our core business, Inflow customers have the peace of mind that they are working with a long-term partner dedicated to providing quality services. In addition to financial stability, providing outsourced IT services is Inflow's core business – it's the only thing we do. Our customers can feel confident that Inflow will be committed to this very line of business for years to come.



Customer Service

Inflow takes service delivery seriously and works very hard to make sure our customers are happy. In a recent third party survey, Inflow received an overall score of 9.2 on a 10-point scale. Our next closest competitor scored a 7.9 on the same survey.

When Inflow customers need support or access they can contact the local NOC where all calls are personally answered in 2 rings or less, 24 hours a day, 7 days a week, by technically savvy operations technicians who are empowered to address almost any issue confronting a customer. Inflow's goal is to limit trouble ticketing and escalation times by empowering our local operations personnel to address as many issues as possible at the local level. This model provides our customers with a high degree of accountability and proactive service.

Experience

Inflow has been providing high quality outsourced IT services for 5 years. Currently, Inflow manages over 750 customer applications across 6 Vertical markets. Inflow has over 125 Gbps of bandwidth capacity and 20 carrier networks under management. We operate over 500,000 Sq. Ft of data center space with 13 dedicated Network Operations centers.

At the same time, Inflow has gained experience in managing infrastructure for companies such as: Comcast Communications, Emerson Electric, Hoover's Online, American Honda, and Charter Communications. Our products are mature and reliable. When it comes to management of mission critical applications Inflow has a solid track record of performance.



Solution

The diagram on page 9 provides a visual overview of the proposed solution. Inflow has quoted datacenter space and managed services to provide the necessary auxiliary services to enable your application:

Cabinet (Data Center Services)

The pictures below show the Denver III Network Operations Center (NOC) and customer cabinets in the datacenter. The datacenter space is adjacent to the NOC and is staffed 24x7x385 with technicians that will support your critical systems.



InflowNet

InflowNet will provide completely redundant connections to the Internet with a 100% availability SLA. The 2 Ethernet cables from the InflowNet switches will terminate in an Inflow provided and managed Catalyst 2912XL switch that is part of the SecureFlow firewall product offering.

Managed Security Services

The SecureFlow switch will be configured for 2 VLANs. One VLAN will provide (red and black cables on the drawing) connectivity to both the web servers and the external firewall interface. The second VLAN will be configured for out-of-band management of the firewall by the SecureFlow engineering team. A custom firewall policy will then be created to ensure controlled and secure access to the servers. All other traffic from the Internet will be blocked. The Cisco 3005 VPN concentrator will allow remote users at stores to dial-up and connect to the Internet using any local ISP service. Once connected, a secure link (encrypted 3-DES) between the remote workstation and the production servers will allow users to upload/download data as required.

Standard AIMS (MonitorFlow)

From the NOC, Inflow technicians and engineers will monitor and troubleshoot problems with your application, operating systems, and hardware 24X7X365. Inflow will also monitor and manage network circuits and all other systems providing critical support to your application. Monitoring services include custom troubleshooting procedures that Inflow engineers will work with you to construct. In the event of an alarm, Inflow will immediately respond and correct the problem.

StorageFlow

Tape backup services will ensure that mission critical data residing on your servers is backed up to tape nightly.



Server Management

Server Management in connection with Standard AIMS (MonitorFlow) services ensures response and support for your servers and applications. Our technicians and engineers document custom troubleshooting procedures so that in the event of an alarm, Inflow can immediately respond and correct the problem. Inflow will also proactively apply upgrades and patches to your systems to ensure application compatibility and security updates are in place.



Customer References

THE REFERENCES BELOW HAVE AGREED TO BE REFERENCES FOR INFLOW'S SERVICE OFFERINGS. PLEASE DO NOT USE THIS LIST FOR ANY OTHER PURPOSES OTHER THAN TO CHECK REFERENCES. THANK YOU.

ELECTRONIC FUNDING GROUP
PAUL MCCLINTON
PRESIDENT
WACO, TX
PHONE: 254-399-8888
EMAIL: CRUNCH@TEXNET.NET

COMPU-CARE MANAGEMENT – INTERNET-BASED SYSTEM FOR FOSTER AND SOCIAL CARE,
HIPAA COMPLIANT
MARGARET WALSH
DIRECTOR IT
AUSTIN, TX – FACILITY
PHONE: 512.219-8025
EMAIL: MWALSH@COMPU-CARE.NET

COMCAST
BILL NEWMAN (EXECUTIVE ASSISTANT: SUSAN @ 856.317.7219)
SR. DIRECTOR
PHILADELPHIA, PA – FACILITY
PHONE: 856.317.7210
EMAIL: BILL_NEWMAN@CABLE.COMCAST.COM

INFOGLIDE SOFTWARE CORPORATION
CHARLES CLENDENEN
CTO
AUSTIN, TX
PHONE: (512) 532-3608
EMAIL: CLENDEEN@INFOGLIDE.COM

HIRE.COM
STEVE DAVIS
CTO
AUSTIN, TX
PHONE: (512) 583-4731
EMAIL: SDAVIS@HIRE.COM



APPENDIX 2(c)
QUOTATION SUMMARY AND PROJECT OVERVIEW



January 10, 2003

Mr. David J. McLaury
 Director, Project Development and Implementation
 Michigan Department of Community Health
 P.O. Box 30479
 400 S. Pine, 7th Floor
 Lansing, MI 48909-7979

Dear Mr. McLaury,

Virtual Alert is the dominant leader in HAN systems for the CDC Bioterrorism Grant program. We have five clients using our technology, whereas no other vendor has more than one. And we are going to extend this lead with several more wins over the next 2 months. One of the main reasons for our leadership is that we are the only vendor selling a true product. With our knowledge from our client base and our ready-to-install product, we can deliver a fully functional HAN, customized with your business rules in 30 to 60 days. No other vendor can come close to matching this with all of our functionality and our unmatched administrative capability.

Virtual Alert would like to extend an offer to The Michigan Department of Community Health (MDCH) to install such a system, with a fully redundant site and full management of these systems. In conversations with several officials from MDCH, we understand that you would want to launch the system with approximately 1800 users, with the flexibility to add approximately 1200 more. You will readily see that the proposed price delivers the most functional, useable and administrate-able HAN solution on the market for far less than a custom development (the only available option) would provide. Combined with the fact that a BTRS installation takes up to one-twentieth the time, and far less risk because the solution is proven, this is a tremendous value.

On the next page, I am attaching a quotation summary and high level timeline for the installation. We look forward to hearing from you and to providing a fast and successful implementation of your Health Alert Network. I will serve as your contract expediter. We have registered on the "MAIN" system and now have Payee# 2752992094.

Best regards,

Andrew F. Trickett
 Chief Operating Officer
 Virtual Alert, Inc.
 Federal TIN: 752992094

Contact Information
 ph 512.732.1214 / cell 512.695.6311/ fax 512.732.1202
 7000 Bee Cave Road, Suite 300
 Austin, TX 78746



Quotation Summary

Virtual Alert Software Licensing			
<i>Description</i>	<i>Units</i>	<i>Rate</i>	<i>Sub Total</i>
Level 4 Users	631	\$495.00	\$312,345.00
Level 2+ Users	2,456	\$120.00	\$294,720.00
		\$145,200.0	
BTRS Server – Production Site	1	0	\$145,200.00
BTRS Server – Backup Site	1	\$45,000.00	\$45,000.00
Communications Server	2	\$35,000.00	\$70,000.00
Pre-discount subtotal			\$867,265.00
Discount on initial installation (on 1 st 4 items)		20%	\$(159,453.00)
Post-discount subtotal			\$707,812.00
Annual maintenance (based on pre-discount)		18%	\$156,103.70
Total for Licenses			\$863,915.70

Professional Services			
<i>Description</i>	<i>Units</i>	<i>Rate</i>	<i>Sub Total</i>
Pre-installation Planning Package	1	\$42,600.00	\$42,600.00
Technical Installation (production + backup)	2	\$14,730.00	\$29,460.00
Training – 5 day package	1	\$10,000.00	\$10,000.00
Co-location setup fee	2	\$3,000.00	\$6,000.00
Subtotal for one-time professional fees			\$80,060.00
Co-location monthly fee (units = 12 months each for two systems)	24	\$6,850.00	\$164,400.00
Total for Services			\$252,460.00

3rd Party Components Billed through Virtual Alert (estimates)			
<i>Description</i>	<i>Units</i>	<i>Rate</i>	<i>Sub Total</i>
Long Distance Charges	12 mos	10k min/ mo @ \$0.05/min	\$6,000.00
Required Hardware			\$94,560.00

Grand Total for Initial Installation and First Year of Operations	\$1,216,935.70
--------------------------------------------------------------------------	-----------------------



Notes on Quotation

- MDCH has indicated that it may purchase 481 Level 4 and 1,386 Level 2+ license upfront. For the period of this contract, Virtual Alert is extending an option to MDCH to purchase an additional 150 Level 4 licenses and an additional 1070 Level 2+ licenses at the same unit costs shown above (with the rates for both discounting and maintenance shown above to apply). The license amounts shown above include those optional licenses, as if they are being exercised.
- The above is a summarized version. A detailed pricing proposal is provided, explaining parameters for every line item.
- The Pre-installation Planning Package includes an estimated \$8000 in travel. Actual travel will be billed using State travel rates.
- Except where noted, the above quotes do not include travel costs, nor the costs of the purchasing vehicle
- The training package includes the provision of a Virtual Alert trainer for 5 full working days, to be utilized as MDCH sees fit. The trainer can manage classroom sizes of 25 maximum. The training discussed will be a combination of 1-2 day training for administrators and MDCH trainers, and ½ to 1 day training for end users.
- MDCH may terminate the co-location arrangement for one or both of the sites, with 30 days advance notice. MDCH must purchase at least 3 months, paid up front.
- The long distance fees are an estimate for budgeting purposes. Actual charges will be billed as incurred, on a monthly basis.
- The required hardware has been provided to MDCH under separate cover.

Installation Project Overview

Virtual Alert has found that our BTRS system can be installed in very short order. All of the functionality that we are proposing already exists today, in productized form. Therefore, the technical installation itself requires only 3-5 days. The aspects that drive the overall timeline are: 1) how quickly the 3rd party hardware and software components can be procured, and 2) how quickly the client can develop the business rules that will govern daily usage of the BTRS system.

Below is an example of what is possible if MDCH is engaged and decisive in determining the business rules.

Day	Milestone
Jan 27	MDCH cuts purchase order
Jan 28	Virtual Alert orders hardware; MDCH/VA commence business rules development
Mar 21	Business rules are developed and documented for tech install team
Mar 24	Hardware arrives, technical installation starts
Mar 28	System is installed and fully useable
Mar 31	Training commences

In order for MDCH to realize such a rapid installation, we are recommending the following approach and guiding principles:



- BTRS makes it simple to change most rules after the initial installation (and to delegate this responsibility to local officials). This fact should drive a bias of speed-over-perfection.
- MDCH should assign a very small working group to make the decisions.
- It is more important to structure the directory and roles than it is to populate the roles – we can get the system up even before all the roles are populated with the right people.
- Similarly, we can populate the roles with incomplete and less-than-100%-perfect data.
- We should strive for simplicity in initial design of every aspect. Let the individual working groups that will use the system make all the customizations later.
- MDCH's initial purchase should focus on the available BTRS functionality, which is already fully compliant with HAN requirements. We can scope additions later, once the initial system is installed and in use.
- We have found that installation can proceed much quicker if Virtual Alert procures the 3rd party hardware and software on a turnkey basis, and operates the system itself.

APPENDIX 2(d)
HARDWARE LISTING



Michigan ISA Server and Root DC Server Configuration – Will need one ISA and one Root DC per site for a total of four (4) machines.

Date: Tue, 21 Jan 2003 13:39:47 GMT

Catalog Number: 4 04

Catalog Number	Description	Product Code	SKU
PowerEdge 1650:	PowerEdge 1650, Intel Pentium III, 1.4GHz w/512K Cache	165140	[220-8606]
Additional Processors:	Single Processor	1P	[311-1193]
Memory:	512MB SDRAM, 133MHz, 4X128MB DIMMs	512M4D	[311-5514]
Keyboard:	No Keyboard Option	N	[310-3281]
Monitor:	No Monitor Option	N	[320-0058]
Power Source:	AC Power Option for Dell PowerEdge 1650	ACPWR	[310-1357]
PCI Riser:	PCI Riser, 1 x 64/1 x 32MHz slots	64BPCI	[430-0289]
First Hard Drive:	18GB 15K RPM Ultra 160 SCSI Hard Drive	18GB15	[340-3598]
Primary Controller:	PERC3-DI, 128MB Battery Backed Cache, 1 Int, 1 Ext Channels- Embedded RAID	ROMB128	[340-3605]
Diskette Drive:	1.44MB Diskette Drive	FD	[340-3612]
Operating System:	No Factory Installed Operating System	NOOS/W2	[310-1261][420-5100]
Mouse:	No Mouse Option	N	[310-0024]
First Network Adapter:	Dual On-Board NICs	OBNICS	[430-8991]
Remote Management:	Dell Remote Access Card, Version III, with Modem	DRAC3	[313-1376]
CD ROM or DVD ROM:	24X IDE Internal CD ROM Drive	CD24X	[313-0317]
Bezel:	Active Bezel Option for Dell PowerEdge 1650	BEZEL	[313-0868]
Hard Drive Backplane:	3 Bay (1x3) Hot Plug SCSI Hard Drive Backplane	1X3BKPL	[311-1586]
Documentation:	Users Manual, Installation and Trouble Shooting Guide on CD	EDOCS	[310-0438]
Second Hard Drive:	18GB 15K RPM Ultra 160 SCSI Hard Drive	18GB15	[340-3598]
Hard Drive Configuration:	On-Board RAID5, 3 drives connected to on-board RAID	MR5	[340-3608]
Chassis Configuration:	VersaRails for Non-Dell 4-Post Rack	3RACKF	[310-1355]
Hardware Support Services:	3Yr Same Day 4Hr Response Parts + Onsite Labor (7 Days x 24 Hours)	W3Y7X24	[900-2962][950-8750]
Installation Support Services:	No Installation	NOINSTL	[900-9997]
Additional Power Supplies:	Redundant AC Power (2nd 275 Watt Power Supply)	RDPWRAC	[310-1358]
Third Hard Drive:	18GB 15K RPM Ultra 160 SCSI Hard Drive	18GB15	[340-3598]
Special Offer:	Special Offer - Save \$200 NOW! Additional \$100 off at check-out with \$2,000	DT200H	[461-3056]
Cluster Status:	No Cluster Info	NOCLUS	[461-1306]

Michigan Public Health Directory Server – Will need one per site or a total of two (2) machines.

Date: Tue, 21 Jan 2003 13:43:28 GMT



Catalog Number: 4 04

Catalog Number	Description	Product Code	SKU
PowerEdge 1650:	PowerEdge 1650, Intel Pentium III, 1.4GHz w/512K Cache	165140	[220-8606]
Additional Processors:	Dual Processor Intel Pentium III, 1.4GHz w/512K Cache	2P140	[311-1585]
Memory:	1GB SDRAM, 133MHz, 2X512MB DIMMs	1GB2D	[311-1896]
Keyboard:	No Keyboard Option	N	[310-3281]
Monitor:	No Monitor Option	N	[320-0058]
Power Source:	AC Power Option for Dell PowerEdge 1650	ACPWR	[310-1357]
PCI Riser:	PCI Riser, 1 x 64/1 x 32MHz slots	64BPCI	[430-0289]
First Hard Drive:	18GB 15K RPM Ultra 160 SCSI Hard Drive	18GB15	[340-3598]
Primary Controller:	PERC3-DI, 128MB Battery Backed Cache, 1 Int, 1 Ext Channels- Embedded RAID	ROMB128	[340-3605]
Diskette Drive:	1.44MB Diskette Drive	FD	[340-3612]
Operating System:	No Factory Installed Operating System	NOOS/W2	[310-1261][420-5100]
Mouse:	No Mouse Option	N	[310-0024]
First Network Adapter:	Dual On-Board NICs	OBNICS	[430-8991]
Remote Management:	Dell Remote Access Card, Version III, with Modem	DRAC3	[313-1376]
CD ROM or DVD ROM:	24X IDE Internal CD ROM Drive	CD24X	[313-0317]
Bezel:	Active Bezel Option for Dell PowerEdge 1650	BEZEL	[313-0868]
Hard Drive Backplane:	3 Bay (1x3) Hot Plug SCSI Hard Drive Backplane	1X3BKPL	[311-1586]
Documentation:	Users Manual, Installation and Trouble Shooting Guide on CD	EDOCS	[310-0438]
Second Hard Drive:	18GB 15K RPM Ultra 160 SCSI Hard Drive	18GB15	[340-3598]
Hard Drive Configuration:	On-Board RAID5, 3 drives connected to on-board RAID	MR5	[340-3608]
Chassis Configuration:	VersaRails for Non-Dell 4-Post Rack	3RACKF	[310-1355]
Hardware Support Services:	3Yr Same Day 4Hr Response Parts + Onsite Labor (7 Days x 24 Hours)	W3Y7X24	[900-2962][950-8750]
Installation Support Services:	No Installation	NOINSTL	[900-9997]
Additional Power Supplies:	Redundant AC Power (2nd 275 Watt Power Supply)	RDPWRAC	[310-1358]
Third Hard Drive:	18GB 15K RPM Ultra 160 SCSI Hard Drive	18GB15	[340-3598]
Special Offer:	Special Offer - Save \$200 NOW! Additional \$100 off at check-out with \$2,000	DT200H	[461-3056]
Cluster Status:	No Cluster Info	NOCLUS	[461-1306]

Michigan BTRS Portal Server – One (1) per site for a total of 2

Date: Tue, 21 Jan 2003 15:36:23 GMT

Catalog Number: 4 04

Catalog Number	Description	Product Code	SKU
Base:	PowerEdge 2650, Intel Xeon 2.8GHz w/512K Cache	265280	[221-1644]
Additional Processors:	Dual Processor Intel Xeon, 2.8GHz w/512K Cache	2P28	[311-2222]



Memory:	1.0GB DDR, 2X512 DIMMS	1GB2D	[311-1618]
Keyboard:	No Keyboard Option	N	[310-3281]
Monitor:	No Monitor Option	N	[320-0058]
First Hard Drive:	36GB, 15K RPM, 1" Ultra3 (Ultra 160) SCSI Hot Plug Hard Drive	36GB15	[340-3940]
Primary Controller:	PERC3-DI, 128MB Battery Backed Cache, 2 Internal Ch- Embedded RAID	ROMB128	[340-3943]
Diskette Drive:	1.44MB Diskette Drive	FD	[340-3961]
OPERATING SYSTEM:	No Factory Installed Operating System	NOOS/W2	[420-5100][310-1261]
Mouse:	No Mouse Option	N	[310-0024]
First Network Adapter:	Dual On-Board NICS	OBNICS	[430-8991]
CD ROM or DVD ROM:	24X IDE Internal CD ROM Drive	CD24X	[313-0317]
Bezel:	Active Bezel Option for Dell PowerEdge 2650	BEZEL	[310-1487]
Hard Drive Backplane:	5 Bay (1x5) Hot Plug SCSI Hard Drive Backplane	1X5BKPL	[340-3932]
Documentation:	Users Manual, Installation and Trouble Shooting Guide on CD	EDOCS	[310-1989]
Second Hard Drive:	36GB, 15K RPM, 1" Ultra3 (Ultra 160) SCSI Hot Plug Hard Drive	36GB15	[340-3940]
Hard Drive Configuration:	On-Board RAID 5, 3 to 5 drives connected to on-board RAID	MR5	[340-3946]
Chassis Configuration:	VersaRails for Non-Dell 4-Post Rack	3RACKF	[310-1714]
Hardware Support Services:	3Yr Same Day 4Hr Response Parts + Onsite Labor (7 Days x 24 Hours)	W3Y7X24	[900-2960][900-2962][950-4649]
Installation Support Services:	No Installation	NOINSTL	[900-9997]
Power Supplies:	Redundant AC Power (2x500 Watt Power Supplies)	REDPWR	[310-1485]
Fourth Hard Drive:	36GB, 15K RPM, 1" Ultra3 (Ultra 160) SCSI Hot Plug Hard Drive	36GB15	[340-3940]
Fifth Hard Drive:	36GB, 15K RPM, 1" Ultra3 (Ultra 160) SCSI Hot Plug Hard Drive	36GB15	[340-3940]
Third Hard Drive:	36GB, 15K RPM, 1in Ultra3 (Ultra 160) SCSI Hot Plug Hard Drive	36GB15	[340-3940]
Special Offers - Dollars Off:	Save \$200 NOW!	DT200	[461-2382]

Michigan Communications Server – One (1) per site for a total of 2

Date: Tue, 21 Jan 2003 15:44:09 GMT

Catalog Number: 4 04

Catalog Number	Description	Product Code	SKU
Base:	PowerEdge 2650, Intel® Xeon™ 2.0GHz w/512K Cache	265200	[220-8929]
Additional Processors:	Single Processor	1P	[311-1193]
Memory:	512MB DDR, 200MHZ, 2X256MB DIMMS	512M2D	[311-1615]
Keyboard:	No Keyboard Option	N	[310-3281]
Monitor:	No Monitor Option	N	[320-0058]
First Hard Drive:	18GB, 15K RPM, 1" Ultra3 (Ultra 160) SCSI Hot Plug Hard Drive	18GB15	[340-3936]
Primary Controller:	PERC3-DI, 128MB Battery Backed Cache, 2	ROMB128	[340-3943]



	Internal Ch- Embedded RAID		
Diskette Drive:	1.44MB Diskette Drive	FD	[340-3961]
OPERATING SYSTEM:	No Factory Installed Operating System	NOOS/W2	[420-5100][310-1261]
Mouse:	No Mouse Option	N	[310-0024]
First Network Adapter:	Dual On-Board NICS	OBNICS	[430-8991]
CD ROM or DVD ROM:	24X IDE Internal CD ROM Drive	CD24X	[313-0317]
Bezel:	Active Bezel Option for Dell PowerEdge 2650	BEZEL	[310-1487]
Hard Drive Backplane:	5 Bay (1x5) Hot Plug SCSI Hard Drive Backplane	1X5BKPL	[340-3932]
Documentation:	Users Manual, Installation and Trouble Shooting Guide on CD	EDOCS	[310-1989]
Second Hard Drive:	18GB, 15K RPM, 1" Ultra3 (Ultra 160) SCSI Hot Plug Hard Drive	18GB15	[340-3936]
Hard Drive Configuration:	On-Board RAID 0, 1 to 5 drives connected to on-board RAID	MR0	[340-3944]
Chassis Configuration:	VersaRails for Non-Dell 4-Post Rack	3RACKF	[310-1714]
Hardware Support Services:	3Yr Same Day 4Hr Response Parts + Onsite Labor (7 Days x 24 Hours)	W3Y7X24	[900-2960][900-2962][950-4649]
Installation Support Services:	No Installation	NOINSTL	[900-9997]
Power Supplies:	Non-Redundant AC Power (500 Watt Power Supply)	NREDPWR	[310-1486]
Special Offers - Dollars Off:	Save \$200 NOW!	DT200	[461-2382]



APPENDIX 2(e)
PRICING PROPOSAL FOR
INITIAL INSTALLATION OF BTRS



Public
Health
Information
Solutions



Pricing Proposal for Initial Installation of BTRS

**Michigan Department of Community
Health**
January 10th, 2003

Virtual Alert, Inc.

7000 Bee Caves Road
Suite 300
Austin, TX 78746

Office (512) 732-1214

Email us at:
info@virtualalert.com

Visit our Web site at:
www.virtualalert.com

Meeting the requirements of HAN and NEDSS



TABLE OF CONTENTS

1	Executive Summary and Overview.....	87
3	General Issues	88
4	Virtual Alert Software Licensing.....	89
4.1	VIRTUAL ALERT SOFTWARE USER LICENSES (ITEMS #1 AND #2)	89
4.2	BTRS SERVER LICENSE (ITEMS #3 AND 4)	90
4.3	VIRTUAL ALERT COMM SERVER (ITEM #5)	90
4.4	PRE-DISCOUNT SUBTOTAL ON VIRTUAL ALERT SOFTWARE (ITEM #6)	90
4.5	SPECIAL ONE-TIME DISCOUNT FOR INITIAL INSTALLATION (ITEM #7)	91
4.6	POST-DISCOUNT SUBTOTAL (ITEM #8)	91
4.7	VIRTUAL ALERT SOFTWARE MAINTENANCE (ITEM #9)	91
5	Installation Project Overview.....	91
6	Pre-installation Planning Package (item #11).....	92
6.1	OVERVIEW	92
6.2	EXAMPLES OF BUSINESS RULES TO BE SET	92
6.3	ROLES PERFORMED BY VIRTUAL ALERT	93
6.4	VIRTUAL ALERT'S VALUE-ADD AND DIFFERENTIATORS	93
6.5	PROPOSED ARRANGEMENT FOR PRE-INSTALL CONSULTING	93
7	Technical Installation (item #12)	93
7.1	OVERVIEW OF THE FULL TECHNICAL INSTALLATION PROCESS	93
7.2	DRIVERS OF TIMING FOR INSTALLATION OF THE SYSTEM	94
7.3	PROPOSED ARRANGEMENT FOR TECHNICAL INSTALLATION	94
8	Training (item #13).....	94
9	Co-Location Services (items #14 and #16)	95
9.1	GENERAL	95
9.2	CO-LOCATION SERVICES PRICING AND DESCRIPTION	96
10	Functionality Discussion	98
10.1	RECOMMENDED OVERALL APPROACH	98
10.2	FUNCTIONALITY LIKELY IN DEVELOPMENT PLAN	99



Executive Summary and Overview

Virtual Alert is very pleased to have the opportunity to provide this proposal to the Michigan Department of Community Health (MDCH). Our understanding is that MDCH desires to improve its information platform capabilities in a way that:

- Leverages a proven system already in use at other jurisdictions;
- Is already fully compliant with current CDC guidelines for HANs;
- Provides a platform to integrate with NEDSS;
- Provides compliance with multiple requirements across the entire Bioterrorism Grant program
- Provides collaboration tools and intelligent alert capabilities to accelerate progress across the entire Bioterrorism Grant program, other MDCH programs, as well as homeland security and emergency management in Michigan
- Provides a platform to eventually integrate with other Public Health data communication & exchange networks (e.g., LRN, EPI-X, etc.)

The Virtual Alert team has unmatched experience in understanding and implementing information technology for Public Health needs, particularly for HAN and NEDSS programs—in fact, we installed the first HAN-compliant system and are a clear leader in NEDSS-compliant systems, Electronic Laboratory Reporting and Smallpox vaccination management tools. We have developed an offering based on a packaged software product, plus services, which can provide an implementation that is faster, higher quality, and more effective than any alternative.

As MDCH will no doubt recognize, Virtual Alert is making a special offer at very attractive pricing for the software and services. The next section presents the specific proposal we are offering. The following sections explain the parameters of each main element. In order to match the functionality and usability of the Virtual Alert offering, MDCH would incur 2-3x the cost in development expense, probably taking well over a year to implement and undertaking great risk of execution.

This offer is good for 60 days from the date on the cover page and I will serve as the contract expeditor on our end. Virtual Alert is the clear leader in providing public health information platform solutions. We do not take this leadership for granted. It would be our great pleasure to add Michigan to our industry-leading and fast-growing list of highly satisfied clients.

Sincerest regards,

Andrew F. Trickett
Chief Operating Officer
Virtual Alert, Inc.
Federal TIN: 752992094



Important Notes on the Price Proposal

- The BTRS system requires 3rd party software and hardware in order to function, be scalable and provide appropriate security and backup. Those elements, along with telephone lines and long distance call charges are included as estimates within this pricing proposal. Virtual Alert is providing basic configuration documentation under separate cover. Long distance charges will be billed at actual cost as incurred, on a monthly basis.
- This proposal is to establish one primary production site which stands “outside” of other MDCH systems. Additionally, we are including provisions for Virtual Alert software and services to install and operate a backup site.
- Subsequent to getting this program underway, MDCH may wish to add custom functionality and/or integrate BTRS into any other systems or applications. That will involve extra software and/or services. Virtual Alert will readily provide pricing for such elements, once it has had a chance to scope the specific requirements involved. Virtual Alert has discussed certain functionality inquiries with MDCH. We will address some of these in the last section of this proposal.
- Detail of the elements that comprise the co-location services fees are provided in a dedicated section within this document.
- The proposal provided herein does not include the costs, if any, for the contracting vehicle to be utilized or applicable sales taxes. MDCH will bear any such costs.
- All professional fees listed herein do not include travel-related expenses. For these, Virtual Alert proposes that the Federal Travel Reimbursement guidelines be utilized.

General Issues

Virtual Alert is providing a quote for MDCH to utilize BTRS primarily for public health officials for the CDC Bioterrorism Grant program. This philosophy applies especially to server licenses. Virtual Alert is going to be very reasonable in acknowledging that response to bioterrorism involves officials from homeland security, public safety / law enforcement, emergency management agencies, EMS, etc. However, Virtual Alert reserves the right to define additional servers/systems as essentially “new clients”, for which the “subsequent license” discounts for server licenses will not apply. The purpose is not to impose unreasonable restrictions. Rather, the purpose is to ensure that Virtual Alert is not being, de facto, forced to support additional, completely different “systems” than the one that has been purchased.

Virtual Alert is willing, within reason, to apply all license fees paid to Virtual Alert under this proposed program to apply to any subsequent enterprise license. And this will apply whether such an arrangement is limited to MDCH/bioterrorism or extended to cover other agencies.

Virtual Alert is willing to enter into an arrangement whereby the source code for BTRS is placed in escrow, so that MDCH can access such code in the unlikely event that Virtual Alert becomes defunct and no buyer of the company, the BTRS product, or the source code has emerged within some reasonable period of time.



Virtual Alert Software Licensing

Virtual Alert Software User Licenses (items #1 and #2)

Client access licenses (CALs) are priced on a per-user basis, which vary depending upon the type of user and the functionality for which they are allowed to utilize. Per discussions with MDCH, this proposal provides 481 users the highest level of functionality currently provided (Level 4) and 1,386 users a more limited usage of the system (Level 2+) (both described immediately below). MDCH users will enjoy rights to use BTRS version 2.0 (see “Software Maintenance” for discussion of future versions). If a future version is shipping by the time the initial installation is performed, our intention is to install the latest available version.

Virtual Alert will not charge MDCH incremental user CALs for backup/hot or test environment sites utilized primarily by MDCH.

MDCH has indicated that it may purchase 481 Level 4 and 1,386 Level 2+ license upfront. For the period of this contract, Virtual Alert is extending an option to MDCH to purchase an additional 150 Level 4 licenses and an additional 1070 Level 2+ licenses at the same unit costs shown above (with the rates for both discounting and maintenance shown above to apply). The license amounts shown above include those optional licenses, as if they are being exercised.

Description of “Level 4” User License

Each user will be placed in the Public Health Directory and assigned the appropriate roles and securities. These users have full access to the functionality provided on the BTRS portal. This includes the ability to access information, publish and edit documents, subscribe to content, fax distribute documents, look up others in the Public Health directory, and participate in discussions based upon the permissions that have been assigned to that user’s roles. Furthermore, they will be able to initiate alerts. They are able to maintain their own profiles through the portal. Administrators can maintain the user profiles, roles and permissions through the portal. They are able to receive alerts via any device that is addressable via SMTP messaging. They can also receive alerts via any telephone through voice alerts and through fax.

Description of “Level 2+” User License

User can maintain their profiles through a web page. Administrators can maintain the user profiles and roles through the portal. They are able to receive alerts via any device that is addressable via SMTP messaging. They can also receive alerts via fax and via any telephone through voice alerts.

As a marketing investment and act of goodwill, Virtual Alert is willing to allow MDCH to utilize a limited number (to be defined by Virtual Alert) of free Level 4 licenses for usage by relevant Canadian officials in border areas (such as Windsor), so that Michigan has the ability to collaborate and communicate with these officials. Virtual Alert is also willing to discuss similar free licenses for bordering U.S. states. Virtual Alert will be evaluating the reasonable probability of being able to make a “new system” sale to any such entities for which we grant the “free seats”.

As far as the purchased CALs, Virtual Alert will certainly allow MDCH to include outside-of-Michigan officials, within reason. This caveat is only to state that Virtual Alert will not allow a major non-Michigan “entity” (a state, a province, or large city) to run its de facto HAN on top of MDCH’s system. The CALs can only be used with a limited number (defined by Virtual Alert) of key, high level officials from border states and countries. The exception to this limitation is that MDCH can put as many tribal officials as it desires, as long as they are members of an Native American nation within Michigan.

MDCH may decide, after the fact, that it wishes to “trade” a certain number of Level 4 for Level 2+ licenses for different mix of user CALs. Virtual Alert is willing to accommodate this, within reason. The intention is that MDCH make these trades on a one-time basis for licenses not yet utilized. Virtual Alert will not support



“churning” of licenses for individuals. Also, Virtual Alert needs to realize the same or greater amount of licensing revenue that it would under the original structure proposed herein.

BTRS Server License (items #3 and 4)

The server license for BTRS is priced on a per-server-installed basis. MDCH will need to purchase at least one (1) server license in order to use BTRS. In order to use BTRS on backup/hot sites and test/training environments, Virtual Alert provides very significant discounts for subsequent server license purchases. This arrangement holds true only for an individual “client”. Virtual Alert reserves the right to interpret whether a subsequent server license is for the same “client” or a new one. Under this specific proposal, MDCH will enjoy rights to use BTRS version 2.0 (see “Software Maintenance” for discussion of future versions) or any future version that is shipping by time of initial installation.

Virtual Alert Comm Server (item #5)

The communications server is the underlying engine that makes it possible to send alerts via phone and fax. There are two reasons why it is sold separately from the BTRS Server License. The first reason is that it is actually an integrated piece of hardware, whereas the BTRS Server License is purely software. The second reason is that some prospective clients have asked for quotations for systems that send only email/SMTTP based alert messages (which BTRS can provide without the comm server).

Comm servers must be purchased for every “system” that exists and must be able to generate alerts. Therefore, we have included two such comm server licenses within this proposal – one for the primary production site, and one for the backup/hot site.

Each comm server comes standard with enablement to support 1 PRI line. If more PRI lines are required, additional hardware for the underlying comm board will be required. We will discuss the cost implications in the separate configuration document.

Pre-discount Subtotal on Virtual Alert Software (item #6)

This amount represents the list pricing for Virtual Alert’s software, as configured in the table above. We strongly believe that this represents very fair and reasonable pricing. We base this upon the direct knowledge of the time and cost that MDCH would incur to build the system itself or to contract with a custom developer to build it (there are no other productized solutions that have all the BTRS functionality). Our BTRS product leverages the work of three such custom build-outs by a sister company, plus knowledge of costs incurred by other jurisdictions that have contracted to have a similar system built. Not only is BTRS a less expensive alternative, it also provides substantially higher value by reducing the risk of the project (given that it is proven). Perhaps most importantly, there is simply no offering that can offer all this functionality in such a dramatically fast deployment – days instead of the greater-than-one-year alternative of a typical custom build.

Nevertheless, Virtual Alert is willing to provide for a special, one-time discount to MDCH for this initial installation, as a good faith investment in developing a relationship by helping MDCH make very fast progress against such an important program and to reflect the significant number of licenses being purchased upfront. Our expectation is that our list pricing, or close to it, will apply to future purchases by MDCH or any other agency in Michigan if licenses are purchased in an “incremental” fashion rather than large blocks or in an enterprise license arrangement. We are applying a 20% discount on all BTRS server licenses and user licenses (items 1-4). We cannot apply discounts to comm servers as they reflect a hard-cost pass-through of a 3rd party vendor’s product that we are integrating into our system.

This discount item will appear as one lump-sum software package on the contracting vehicle, rather than in separate line items. If MDCH desires a separate arrangement, Virtual Alert will be very flexible in accommodating MDCH’s needs.



Special One-time Discount for Initial Installation (item #7)

This item will appear as a temporary, special, one-off promotion on the contracting vehicle. MDCH and Virtual Alert may need to be diligent and skillful in timing the appearance of this promotion on the contracting vehicle.

Post-discount Subtotal (item #8)

As stated previously, the discount will be reflected in a special SKU on the contract vehicle. This amount is provided for convenience purposes.

Virtual Alert Software Maintenance (item #9)

Maintenance of the BTRS software for this configuration of server and user licenses is priced at 18% (annual rate) of the list price of total Virtual Alert license fees in effect (reflected in item 6). It is paid upfront and on an annual basis. Similar to the majority of typical enterprise COTS product packages, purchase of the maintenance program entitles MDCH to multiple privileges:

- Rights to upgrade to subsequent versions of BTRS with no extra license fees
- Basic support for issues with the software product
- Rights to participate in the BTRS User Group

This summary is for convenience purposes only.

Installation Project Overview

Virtual Alert has found that our BTRS system can be installed in very short order. All of the functionality that we are proposing already exists today, in productized form. Therefore, the technical installation itself requires only 3-5 days. The aspects that drive the overall timeline are: 1) how quickly the 3rd party hardware and software components can be procured, and 2) how quickly MDCH can develop the business rules that will govern daily usage of the BTRS system and assemble the data required for the public health directory.

Below is an example of what is possible if MDCH is engaged and decisive in determining the business rules.

Day	Milestone
January 27	MDCH has cut purchase order for all elements
January 28	Virtual Alert orders hardware; MDCH/VA commence business rules development
March 21	Business rules are developed and documented for tech install team
March 24	Hardware arrives, technical installation starts
March 28	System is installed and fully useable
March 31	Training commences

In order for MDCH to realize such a rapid installation, we are recommending the following approach and guiding principles:

- BTRS makes it simple to change most rules after the initial installation (and to delegate this responsibility to local officials). This fact should drive a bias of “80% accuracy delivered fast is preferred over 100% accuracy delivered slow”



- MDCH should assign a very small working group to make the decisions. This group needs to have the qualifications and authority to make the decisions.
- It is more important to structure the directory and roles than it is to populate the roles – we can get the system up even before all the roles are populated with the right people.
- Similarly, we can populate the roles with incomplete and less-than-100%-accurate data (within reason, obviously).
- We should strive for simplicity in initial design of every aspect. Let the individual working groups that will use the system make the bulk of customizations later.
- MDCH's initial purchase should focus on the available BTRS functionality, which is already fully compliant with HAN requirements. We can scope additions and modifications later, once the initial system is installed and in use.
- We have found that installation can proceed much quicker if Virtual Alert procures the 3rd party hardware and software on a turnkey basis, and operates the system itself.

Pre-installation Planning Package (item #11)

Overview

Pre-Install Planning provides valuable guidance for MDCH to develop the “business rules” for how the system will actually be used on a day-to-day basis. The nature of this work is that producing deliverables is driven overwhelmingly by the client’s engagement, availability and speed of decision-making. Therefore, Virtual Alert provides and prices these services on a package-of-set-hours basis. We are happy to accommodate any arrangement that MDCH prefers. Our prescriptive recommendation is included below.

Examples of Business Rules to be Set

- Determine which participants, from which public health partners, will be involved, over what period of time.
- Define the Public Health Roles that will be utilized by MDCH, which can be quite different than many existing “organization” roles. Virtual Alert has strong working relationships with groups that are defining emerging “standards” for roles. However, MDCH will probably want to create custom roles, which are appropriate for the unique roles and taxonomy within your jurisdiction.
- Determine who will have full administration authority and capabilities for the Public Health Directory.
- Construct the taxonomies for the folder and category structures within the document library.
- Determine the various roles for individual participants and/or Public Health roles, regarding the document management functionality on the BTRS portal—“read only” vs. “authorship privileges” vs. “administration capabilities”.
- Set the ground rules for sending alerts—define “alert-worthy events”, set roles for who can send/receive different types of alerts, and to whom.
- Define the various types of alerts—types of alerts; define a “High” vs. “Medium” vs. “Low” alert.



Roles Performed by Virtual Alert

- Manage the process by which MDCH develops its business rules.
- Provide templates to support the process.
- Provide insights into best practices and lessons-learned for establishment of such business rules.

Virtual Alert's Value-add and Differentiators

- During our 4 years of experience in dealing with these issues, we have seen and developed best practices that we can share with MDCH. We have also encountered many pitfalls that we can help MDCH avoid.
- The Virtual Alert team also has specialized experience in business process development and management of such projects, both within and outside of the public health industry.

Proposed Arrangement for Pre-install Consulting

- On-site consulting to organize, commence and prosecute the effort.
- Off-site consulting, while the MDCH team gathers the essential data and internally deliberates the major decisions.
- The mix of the two will depend on MDCH availability, speed in decision-making, and desired calendar for executing deliverables.
- The amount shown for this package includes an estimated \$8000 for travel. Actual travel will be billed at cost per FTR.

Technical Installation (item #12)

Overview of the Full Technical Installation Process

Virtual Alert will provide a pre-install checklist for MDCH to understand all of the components involved, and for MDCH to commence preparation of the technical environment (i.e., 3rd party components). There will be a preparatory conference call between MDCH technical staff and Virtual Alert's installation team – to ensure that MDCH understands all requirements, so that the environment is ready when the installation team commences its work.

Once MDCH has properly prepared all items on the checklist, the Virtual Alert installation team arrives on site to fully configure the hardware, software, and networking components. This team will also populate the Public Health Directory with the data assembled by the MDCH team. We fully expect, and welcome, that MDCH staff participate in this installation process, to ensure "knowledge transfer". In fact, we see this participation as an effective and inexpensive way to conduct de-facto training for MDCH's engineering staff.

Upon the completion of the on site visit, the Virtual Alert representative will generate the necessary documentation to provide a trouble free implementation of the system.



As this proposal assumes Virtual Alert will be maintaining both the primary production system and the backup system, it is appropriate that we discuss the environment in which these systems will reside. These will be discussed within the Co-Location Services section. In general, Virtual Alert intends to place the systems within data center partners' facilities. The current plan is to place the primary production site at SureWest's facility in Sacramento, with the backup at InFlow's facility in Austin. These are both cities where Virtual Alert has offices and staff. We readily welcome MDCH to conduct some level of due diligence on these data centers, in order to become more comfortable with the arrangement. We are confident that MDCH will conclude that these facilities provide the high quality environment expected of a first class data center regarding security, service, power backup, phone/ISP provision, etc.

Drivers of Timing for Installation of the System

Once the required components are procured, the business rules have been established and the required data gathered, the technical installation activities can proceed very quickly. We have found that the configuration and setup of the hardware and software components for a "straightforward" installation takes approximately 3-5 business days for each system if there are no major problems with any of the procured components.

Proposed Arrangement for Technical Installation

- Off-site preparation to develop checklist and guide MDCH tech team.
- On-site installation.
- Off-site documentation for MDCH IT and VA customer support teams

Training (item #13)

Virtual Alert offers training for end users, portal administrators, clients' trainers (train-the-trainer) and engineers. Virtual Alert is highly flexible in designing packages that meet the client's specific needs and desires. As a prescriptive recommendation, Virtual Alert is proposing a 5 day package that combines many of these elements:

- 2 days of training for portal administrators and MDCH trainers
- 3 days of standard training for a core subset of the initial end users

Virtual Alert will provide a trainer and standard training materials (primarily the BTRS user's manual). The fees shown above do not include extra training aids that MDCH may desire. MDCH will be responsible for managing logistics of arranging training (such as scheduling specific individuals to be trained) and providing a suitable location and facilities (especially, computers with high speed internet access for each trainee).

Training of MDCH Trainers and Portal Administrators

- Virtual Alert will provide an individual to train -- at a location of MDCH's choosing -- MDCH staff who will serve as trainers of subsequent MDCH users and those who will serve as portal administrators.
- This will consist of two days of training that will cover assigning roles, assigning security levels, managing folders, managing user profiles, managing passwords, taxonomy and many other items.
- The training will be comprehensive in nature and will provide the participants the knowledge that is necessary to administer the BTRS system and to train end users to use the system.



End-user Training

- Virtual Alert will provide for a trainer to be at the customer location to provide training for three days.
- The format and recommended utilization of these three days can be organized however the client would like. Virtual Alert recommends:
 - Classes of no more than 25 people
 - Each class should last at least a half day

Co-Location Services (items #14, and #16)

General

There are a number of benefits to having your BTRS system co-located and operated by Virtual Alert. First, the Virtual Alert co-location and operation service will bring MDCH's system on line in the shortest time possible. Second, the Virtual Alert team that will be operating your system has the most experience running and operating HANs in the country. Third, any required customizations can be quickly developed, tested and integrated by the Virtual Alert team operating MDCH's system. Finally, while system training and evaluation is occurring, the Virtual Alert team will be able to provide additional capacity planning and usage expertise.

One of the critical areas for a successful system is the administration of the portal. The Virtual Alert team has unmatched experience in administering the system and is currently doing so for California, Los Angeles County, Department of Health and Human Services, Office of Public Health Preparedness (OPHP) and a working group of the Lab Response Network. Additionally, we are about to start providing these services to the Commonwealth of Massachusetts.

Some points of clarification regarding the co-location arrangement:

- This is not an ASP or subscription arrangement. MDCH owns all of the software, hardware and networking components that it is procuring within this proposal. Virtual Alert is only managing the system on MDCH's behalf. Thus, there is no danger that MDCH will lose what it has procured if future-funding streams cannot support the ongoing arrangement.
- MDCH must still purchase the hardware and 3rd party software components required to support the BTRS system.

Virtual Alert intends to place the systems within data center partners' facilities. The current plan is to place the primary production site at SureWest's facility in Sacramento, with the backup at InFlow's facility in Austin. These are both cities where Virtual Alert has offices and staff. We readily welcome MDCH to conduct some level of due diligence on these data centers, in order to become more comfortable with the arrangement. We are confident that MDCH will conclude that these facilities provide the high quality environment expected of a first class data center regarding security, service, power backup, phone/ISP provision, etc.



Co-Location Services Pricing and Description

The table below details the unit pricing reflecting the cost of co-location services for managing a single system. The Site Setup Charge is a one-time fee. All others are paid on a monthly basis.

In order to reconcile this table to the main price proposal table, there are two adjustments to make:

- As Virtual Alert is proposing to manage both the primary production system and the backup site, we are applying two units against all line items
- Virtual Alert typically provides proposals that reflect all project fees for the entire first year of operation

The end result is these two adjustments is that MDCH will incur two site setup charges and 24 “units” of projected monthly co-location expenses in the first year of operation.

<i>One-time Expenses per Site</i>			
Item	Unit	Price	Extended Price
Site Setup Charge	1	\$3,000.00	\$3,000.00
Total One-time Expenses per Site			\$3,000.00

<i>Monthly Recurring Expenses per Site</i>			
Item	Unit	Price	Extended Price
Location Expense for pilot system	1	\$1,200.00	\$1,200.00
Internet Access, .5 - 2.5 Mbps Burstable, 95%*	1	\$750.00	\$750.00
Internet Access, 1.0 - 3.0 Mbps Burstable, 95%*	0	\$1,350.00	\$1,350.00
Internet Access, 2.0 - 10.0 Mbps Burstable, 95%*	0	\$2,700.00	\$2,700.00
System Services and Maintenance	1	\$2,100.00	\$2,100.00
Managed Security Devices	1	\$1,100.00	\$1,100.00
Administrative Review	1	\$1,700.00	\$1,700.00
Total Recurring Expenses per Site			\$6,850.00

Services denoted by an asterisk “*” are invoiced based upon usage. Customer's Monthly Recurring Charge will vary depending on usage. The Monthly Recurring Charge set forth above for such usage based Service(s) is the minimum charge that may be assessed in any month.



Location Expense

The location expense provides for the secure facility in which the system will be housed. This facility provides the power needed to run the system, as well as an environment control system to maintain the optimal operating parameters for the system 24 hours a day, 7 days a week. Virtual Alert staff has 24x7 access to the location and can escalate to the co-location service provider.

Internet Access

Virtual Alert will provide for Internet connectivity in a metered fashion. The quotation above is for .5Mbps nominal that is burstable to 2.5Mbps. This means that during daily use the system will be running at .5Mbps but when an event drives use of the system up the system will accommodate for the added load by broadening the potential bandwidth to 2.5Mbps. This is billed at the 95th percentile. This means that there are frequent readings of the bandwidth that is being used and the client is billed at the average load over 95% of the time. With the number of users that MDCH will initially put onto the system, we anticipate that it would be difficult for MDCH to overload the .5Mbps that will be available. In the event that more bandwidth is needed, MDCH will be billed commensurate with the load.

Virtual Alert will provide monthly usage analysis to MDCH and review this with your system team. This will provide vital feedback to assess the success of the system, and will facilitate capacity planning.

System Services and Maintenance

Virtual Alert will monitor the applications that are used by the system to ensure that they are kept up to date and running properly. Virtual Alert will not add any updates or fixes without first verifying that they will not affect the system negatively, by testing the updates in Virtual Alert's test environment. This will be true for all of the applications that are loaded on the system, including the BTRS software.

Virtual Alert will backup the system once a day on an eight-week rotation. This will consist of full backups twice a week and incremental backups the other days. Once every rotation, Virtual Alert will run a full backup that will be stored in a remote location – away from where the system resides. This external backup can be used for Disaster Recovery or Operational Recovery purposes. Virtual Alert can ship tapes to MDCH for a nominal extra fee.

Virtual Alert will monitor the entire system to ensure that it is constantly running at its peak performance. This will include providing reports and data to MDCH about the system's performance and use. Further, Virtual Alert will monitor the overall health of the system and attempt to identify potential problems before they impact the day-to-day use of the system.

Manage Security Devices

Virtual Alert will ensure that the Cisco PIX, Microsoft Internet Security and Accelerator server and Cisco 3550 VLANs are kept up to date and monitored so that they will continuously provide the highest possible level of security for MDCH's system. When combined with the Server Certificate to enable SSL-128 bit encrypted sessions, as per CDC Guidance, this provides transport level security to be available from the SSL Certificate provider. Virtual Alert understands that the information on MDCH's HAN system is potentially sensitive and thus must be protected from unauthorized intrusion. Further, the proliferation of denial of service and other attacks on systems requires that the system be prepared to automatically fend off attacks that would prevent the use of the system. Virtual Alert will monitor the security systems and prevent these attacks from having an impact on the system.



Administrative Review

Virtual Alert will provide monthly reports organized in such a way that a non-technical person can understand. The reports will cover uptime, problems encountered, enhancements made, backups executed, usage levels and other information so that MDCH will clearly understand the health and utilization of the system.

The complete reports will be posted to the system in a designated folder for easy review. Virtual Alert will also make itself available for conference calls, if so desired by MDCH, to discuss the individual reports.

Fee Arrangements

MDCH must purchase at least 3 months of co-location service on both sites. After that point, with 30 days advance notice, it may cancel the co-location services on one or both of the sites.

Long Distance Charges (item #18)

The cost shown is an estimate for long distance charges that may be incurred by MDCH as the result of initiating telephonic/fax alerts or the distribution of portal documents via fax from the BTRS portal. These costs will be billed, as incurred on a monthly basis.

Functionality Discussion

Recommended Overall Approach

Our understanding is that MDCH is keenly interested in getting the HAN installed as fast as possible. It also has some desires for functionality that may not be provided, out-of-the-box, with a “standard” BTRS deployment. In order to balance these two desires, Virtual Alert proposes that we take the following overall approach.

First and foremost, MDCH and Virtual Alert should focus on getting BTRS installed, with its currently available functionality, as fast as possible. BTRS is very functionally rich, meets all relevant CDC requirements and provides the vast majority of what we understand that MDCH needs and desires of its HAN. We advocate that our joint team not focus on anything else until this initial installation is well underway. An additional benefit of this focus is that the core collaboration functionality in BTRS can actually enable the joint team to manage the following steps.

The second step would be to address functional requests that Virtual Alert would classify as “enabled by the underlying comm board but not yet fully integrated into BTRS”. Given that MDCH has stated a preference for Avtex CityWatch to be used as the underlying comm board, this presents a lot of interesting options for MDCH. CityWatch is a very functionally rich product. There may be certain functionality that MDCH decides doesn’t need to be “fully integrated” into the directory access controls and web browser interfaces that BTRS can provide (or at least, the integration doesn’t need to happen in the immediate term). An illustrative example MAY be the provision of telephonic conference bridges. In these cases, it could be a very simple matter to make this functionality “immediately” available with little or no incremental effort from Virtual Alert and/or Avtex. But Virtual Alert would like to stress that it needs to engage in detailed discussions with MDCH to understand the needs and to weigh the options available.

The third step would then be to prioritize and assess the remaining requirements. Then Virtual Alert will provide an initial response to each item that will generally classify each item into one of the following broad categories:



- The item already is on the BTRS development plan or Virtual Alert is willing to add the item for MDCH's benefit – thus, MDCH would be already getting the functionality as one of its many benefits provided by the software maintenance contract. We will also provide a projected timeline for when the functionality will be formally released. Illustrative examples are provided below in the next section
- The item is not on the development path, but is “straightforward enough” that Virtual Alert can readily provide a proposal for providing the item on a custom development basis
- The item is not on the development path and the considerations are complex, where there are many options of varying impact on BTRS, other systems, as well as very different 3rd party hardware and software requirements. An illustrative example may be scoping the many options for how MDCH can send out a very widely distributed alert (say, to all physicians in Michigan)

Virtual Alert has received a preliminary list of items from MDCH. Obviously, we need to go through the prioritization/assessment effort described above (“the third step”) before we can provide a definitive response to this list. In the spirit of being responsive, Virtual Alert's very preliminary assessment is that a substantial number of the items are either: 1) already available in BTRS, 2) are already on the dev path or would be added if MDCH accepts this proposal, or 3) not on the dev path but look very inexpensive to quickly provide on a custom basis.

Functionality Likely in Development Plan

There are several items on MDCH's functionality list are already anticipated for inclusion into Virtual Alert's development plan. We would like to stress that we would need to engage in detailed discussions to define the exact requirements and capabilities that MDCH is seeking and compare that to the definitions taking shape in the current development plan. In many cases, we should be able to “fully” accommodate MDCH's desires. In others, we may only be able to partially fulfill them in “short order”. In the spirit of being responsive, Virtual Alert can express with a high degree of confidence, that the following capabilities are already scheduled to be provided in the next few releases of BTRS:

- Ability to activate, from a telephone, an alert to a pre-set list of roles and/or individuals
- Ability to utilize .wav files for pre-recorded or recorded messages for telephonic alerts
- Incorporating more of the existing capabilities of the underlying comm board into the BTRS environment. Examples:
 - conference calling
 - “telephone survey”
 - various options for terminating alert sequence (example: stop after getting confirmations from xx number of alertees)
 - prioritize certain roles and/or individuals for alerting
- Automation of routing and BTRS alert activation for CDC alerts



APPENDIX 2 (f)

ESTIMATION TEMPLATE FOR 3RD PARTY HARDWARE AND SOFTWARE



Estimation Template for 3rd Party Hardware and Software

Driving Assumptions	
License Type	Units
User CALs	2500
Server Systems	2
Redundancy Requirements on specific items	none

Hardware Requirements				
Component	Units per Server System	Total Units Needed	Rate	Component Total
MISA Server	1	2	\$6,200.00	\$12,400.00
PHDir Server	1	2	\$6,500.00	\$13,000.00
Root/Security DC	1	2	\$6,500.00	\$13,000.00
BTRS Portal Server	1	2	\$7,940.00	\$15,880.00
Comm. Server	1	2	\$6,200.00	\$12,400.00
Additional Comm Boards	0	0	\$5,000.00	\$0.00
Cisco PIX 515	1	2	\$3,200.00	\$6,400.00
Cisco 3550 Switch	1	2	\$3,800.00	\$7,600.00
Protected Exchange (Opt.)	0	0	\$6,500.00	\$0.00
PRI lines -- annual cost	1	2	\$5,940.00	\$11,880.00
KVM	1	2	\$500.00	\$1,000.00
Cabling	1	2	\$500.00	\$1,000.00
			Subtotal	\$94,560.00

Microsoft Software Requirements				
Component	Units per Server System	Total Units Needed	Rate	Component Total
ISA Enterprise	1	2	\$4,613.13	\$9,226.26
SharePoint Server	1	2	\$3,150.07	\$6,300.14



SharePoint CAL	2500	2500	\$56.54	\$141,350.00
SPS Internet Connector	1	1	\$25,000.00	\$25,000.00
W2K Adv Server	5	10	\$1,889.92	\$18,899.20
W2K CAL	2500	2500	\$23.45	\$58,625.00
SQL Enterprise	1	2	\$15,483.90	\$30,967.80
Exchange 2000 Enterprise	0	0	\$3,999.00	\$0.00
Exchange 2000 CAL	0	0	\$67.00	\$0.00
MS Advantage Maint.				\$84,206.84
			Subtotal	\$374,575.24

Anti-Virus, Backup and SSL Certificate				
<i>Component</i>	<i>Units per Server System</i>	<i>Total Units Needed</i>	<i>Rate</i>	<i>Component Total</i>
Veritas Backup-Exec Advanced Server	1	2	\$1,195.00	\$1,195.00
Veritas Remote Agent-3pack	1	2	\$695.00	\$695.00
Veritas Exchange Agent	0	0	\$795.00	\$0.00
Veritas SharePoint Agent	1	2	\$795.00	\$795.00
Veritas SQL Agent	1	2	\$795.00	\$795.00
Trend Micro Interscan Web Protect	1	2	\$290.00	\$290.00
Trend Micro Server Protect	5	10	\$675.00	\$3,375.00
Trend Micro Portal Protect	1	2	\$600.00	\$600.00
EnTrust SSL Certificate	1	2	\$150.00	\$150.00
			Subtotal	\$7,895.00

GRAND TOTAL FIXED COSTS AND 1ST YEAR OF ONGOING COSTS	\$477,030.24
--------------------------------------------------------------	---------------------



PO Box 2985
La Jolla, CA 92038
Phone: 512-653-3200
Email: eric.shaffer@virtualalert.com

Comments

assuming that all are "internal users" for Microsoft estimations
primary production site + backup site

MDCH may desire 2 servers per system?

May consider as user base grows

Driven by optional protected Exchange component: n/a for MDCH
Ongoing cost; option for growing as user base grows

Driven by number of ISA servers
Driven by number of BTRS servers



Worst case scenario: shouldn't need CALs for all
Need for current and future "external" users
Driven by number of total servers
Need to investigate need and rate with Microsoft
Driven by number of PHDir servers
Driven by optional protected Exchange component: n/a for MDCH
Driven by optional protected Exchange component: n/a for MDCH
Annual fee

Cost of backup package for first server
Cost of backup package for the 2nd/3rd/4th server
Driven by optional protected Exchange component: n/a for MDCH

Driven by number of total servers

Annual fee



APPENDIX 2 (g) CONFIGURATION SPECIFICATION FOR MDCH



Configuration Specifications for MDCH

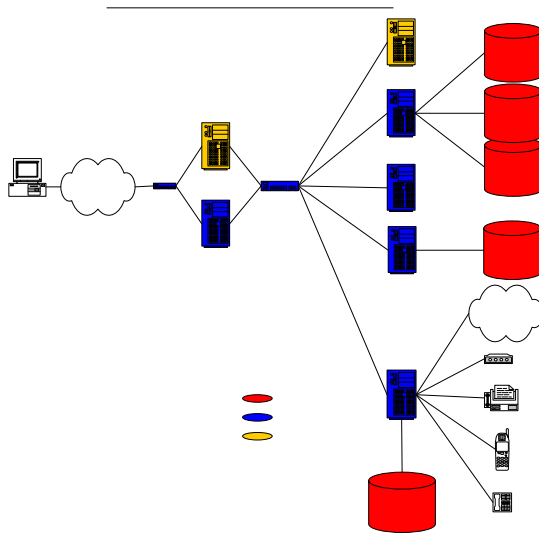
This document provides graphical description of the systems and software that Virtual Alert recommends for the BioTerrorism Readiness Suite, as well as specs for the majority of those components. It also discusses optional items.

Based upon the recommended configurations for MDCH, for both the primary and backup sites to be operated by Virtual Alert, we have attached a spreadsheet that explains the cost drivers. These prices were generated using easily available retail pricing from a top-tier hardware manufacturer and top-tier resellers of the relevant 3rd party software components. They may not reflect more favorable pricing that MDCH may be able secure through its available sources, contracts and purchasing mechanisms. They reflect estimates of what Virtual Alert will bill MDCH if it will manage the procurement process.

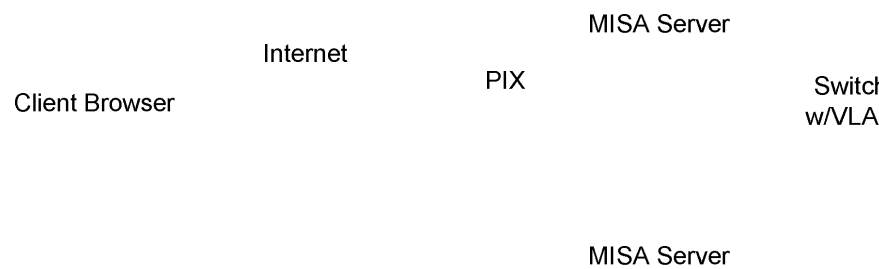
These configurations reflect the standard configurations which we believe have proven quite satisfactory for many other clients' needs. It is possible that specific MDCH requirements will require additional components or additional units of existing components. There are two prominent illustrative examples. First, MDCH's requirements of the co-location services SLA may require Virtual Alert to incorporate further redundancy into each system (the primary production site and the backup site) by purchasing more servers (with the associated costs in 3rd party software). Second, MDCH may demand a higher level of performance for telephonic/fax alerting than the standard configuration can theoretically support – this may involve more of the listed telephonic components or a completely different architectural approach.

Virtual Alert has dedicated a significant amount of time and effort to ensure that the “recommended” configurations and software packages will provide the functionality, sustainability, and security that is required of a system such as this. We also appreciate that many jurisdictions have standards that they would like to adhere to, and in most cases Virtual Alert as been able to accommodate these changes to our suggestions. The above diagram and descriptions are simply a way to outline the items that are needed to provide the desired functionality. Virtual Alert is also developing our future upgrades and modules to work within an environment like the one above, so that future hardware and infrastructure needs are minimized.

The following graphic will be utilized throughout this document as a guide to the various types of hardware and software components of a standard configuration.



Virtual Alert BTRS Conceptual Archite





Hardware Components

Below are listed the recommended specifications for all relevant server hardware. Other hardware elements are listed at the end of this "Hardware" section.

MISA Server

Rack Mountable, 2U Form Factor
 Intel Xeon Processor, 2.6GHz
 512MB RAM on 2 DIMMS
 Windows 2000 Advanced Server
 Internal CD ROM
 Internal Floppy
 Redundant Power Supplies
 Rails for mounting in an Industry Standard 4 post rack
 RAID Controller Capable of RAID 0, 1, or 5
 Hot Swappable hard drives backplane
 Qty. 2 – 18GB, 15k RPM hard drives
 3yr, Same day, 4hr response, 7X24 parts and on-site labor
 Qty. 2 Network Interface Cards
 Mouse and Keyboard Cables

Public Health Directory and Root DC Servers *(two separate servers)*

Rack Mountable, 2U Form Factor
 Intel Xeon Processor, 2.6GHz
 512MB RAM on 2 DIMMS
 Windows 2000 Advanced Server
 Internal CD ROM
 Internal Floppy
 Redundant Power Supplies
 Rails for mounting in an Industry Standard 4 post rack
 RAID Controller Capable of RAID 0, 1, or 5
 Hot Swappable hard drives backplane
 Qty. 3 – 18GB, 15k RPM hard drives
 3yr, Same day, 4hr response, 7X24 parts and on-site labor
 Qty. 2 Network Interface Cards
 Mouse and Keyboard Cables



Virtual Alert BTRS Server

Rack Mountable, 2U Form Factor
 Qty. 2 - Intel Xeon Processor, 2.6GHz
 1GB RAM on 2 DIMMS
 Windows 2000 Advanced Server
 Internal CD ROM
 Internal Floppy
 Redundant Power Supplies
 Rails for mounting in an Industry Standard 4 post rack
 RAID Controller Capable of RAID 0, 1, or 5
 Hot Swappable hard drives backplane
 Qty. 5 – 18GB, 15k RPM hard drives
 3yr, Same day, 4hr response, 7X24 parts and on-site labor
 Qty. 2 Network Interface Cards
 Mouse and Keyboard Cables

Virtual Alert Communications Server (Hardware)

Rack Mountable, Must accommodate 4 full size PCI cards
 Intel Xeon Processor, 2.6GHz
 512MB RAM on 2 DIMMS
 Windows 2000 Advanced Server
 Internal CD ROM
 Internal Floppy
 Redundant Power Supplies
 Rails for mounting in an Industry Standard 4 post rack
 RAID Controller Capable of RAID 0, 1, or 5
 Hot Swappable hard drives backplane
 Qty. 2 – 18GB, 15k RPM hard drives
 3yr, Same day, 4hr response, 7X24 parts and on-site labor
 Qty. 2 Network Interface Cards
 Mouse and Keyboard Cables

Other Hardware Items

Cisco PIX 515E (Rack Mountable)
 Cisco 3550 Switch (Rack Mountable)
 PRI Line
 KVM (Rack Mountable)
 Cabling

Comments

The standard spec for Comm Servers requires 4 full size PCI card slots. This is a requirement if the customer would like to be able to accommodate the fully supported 96 telephone ports. Each card supports one PRI line and each PRI line has 24 ports. If the customer does not see a need for 4 cards, then a chassis that supports fewer cards is acceptable. Many 2U chassis support up to 3 full size cards -- if 72 ports is acceptable to MDCH, then these would work well and possibly save money. The limitation would then only be realized if MDCH grows out of the ability of 72 ports. Given the potential future scale up that has been discussed, we recommend 4 card machines.

3rd Party Software Components



The following diagrams describe how 3rd party software elements are utilized within the configuration. 3rd party software can be categorized into three major vendors:

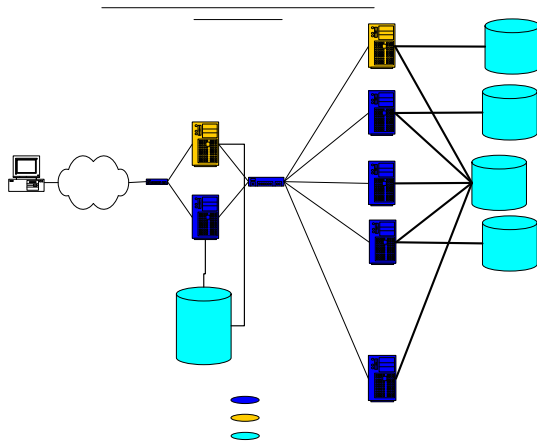
- Microsoft
- Veritas
- TrendMicro and SSL Certificate software

We will use three separate diagrams and subsections to describe and discuss each one. As with the hardware, we are describing itemized components.

Microsoft

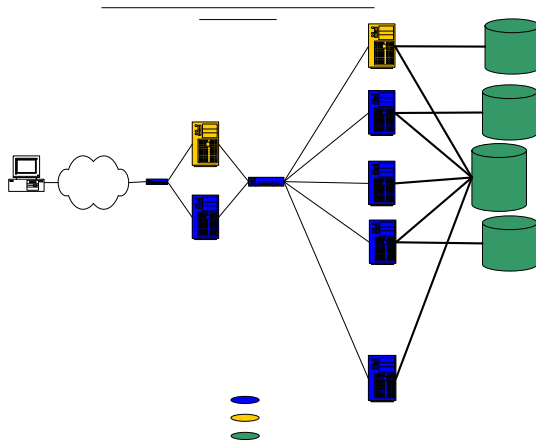
The diagram immediately below provides a graphical description of the roles for Microsoft software within the standard configuration.

- Each server requires a copy of Windows. The version we strongly recommend is Windows 2000 Advanced Server.
- A Windows User CAL is required for every user who will reside in the directory (which leverages Microsoft Active Directory Services). There are no duplicate costs for the backup site.
 - We are presenting a worst case scenario (all users require a new CAL) at the full rates shown
 - MDCH may current ownership and licensing rights such that many users don't need a CAL (because they already have one), and/or a reduced rate can be realized to just have usage of Active Directory
- Each MISA server requires a copy of ISA Enterprise.
- Exchange server licenses and CALS are used only if MDCH wanted to incorporate Exchange for a special secure email or to leverage its instant messaging, conference calling or other capabilities. As has been discussed with MDCH, we are not using it in this initial installation. It may or may not be leveraged down the road.
- Each Public Health Directory server requires a copy of SQL Enterprise.
- Each BTRS Server requires SharePoint 2001 server license
- The requirement for SharePoint CALs requires investigation:
 - There is an Internet Connector license which requires a flat fee and allows for unlimited usage by "external" users
 - Users judged to be "internal" to the purchasing entity require a CAL
 - In the interests of being conservative, the attached spreadsheet assumes that all 2500 users require a CAL and that MDCH will also purchase the Internet Connector license
 - MDCH may have licensing arrangements with Microsoft that result in less cost. Also, it is likely that not all users will be "internal" ones.
 - As Virtual Alert will have responsibility for co-location maintenance, we require that MDCH purchase the Microsoft Advantage Maintenance program to cover all Microsoft software.



Virtual Alert BTRS Conceptual Architecture

The diagram illustrates a network topology. On the left, a 'Client Browser' is connected to an 'Internet' cloud. The 'Internet' cloud is connected to a 'PIX' firewall. The 'PIX' firewall is connected to a 'MISA Server'. The 'MISA Server' is connected to a 'Switch w/VLAN'. The 'Switch w/VLAN' is connected to another 'MISA Server'. The 'Switch w/VLAN' is also connected to a 'Microsoft Internet Security and Accelerator (Enterprise)' device.

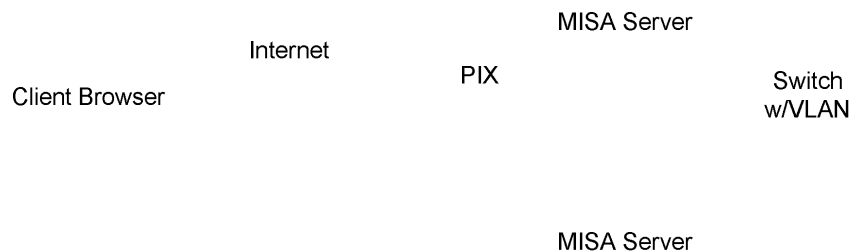


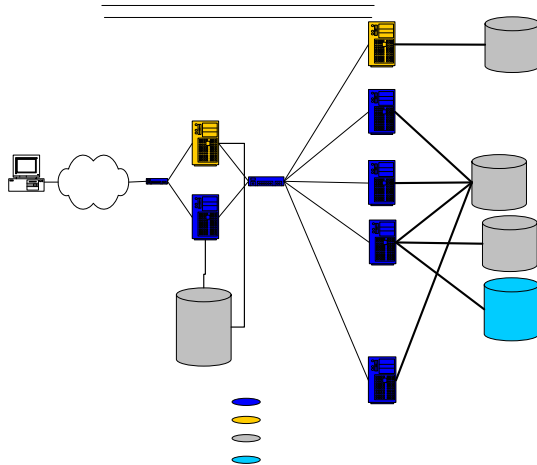
Veritas

Virtual Alert BTRS Conceptual Architecture Veritas Software

The diagram immediately above provides a graphical description of the roles for Veritas software within the standard configuration. For each of the described components, one copy is required for each site:

- Backup Exec. Advanced Server is required for the servers that hold data (optional Exchange, Public Health Directory, Root DC, BTRS, Comm)
 - The first server is covered at full rate
 - The other three servers can be covered by a Remote Agent 3-pack
- If an Exchange Server were being leveraged – which is not the case in this configuration – Veritas Exchange Agent would be used for that server
- The Public Health Directory requires SQL Agent and Open File Option
- The BTRS Server requires SharePoint Agent



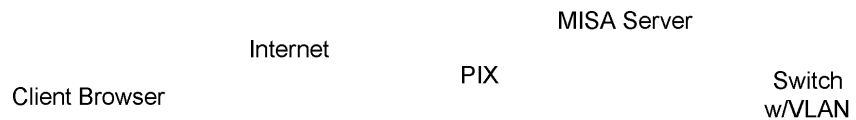


Virtual Alert BTRS Conceptual Architecture TrendMicro and Secure Socket Layer Certificate

TrendMicro and SSL

The diagram immediately above provides a graphical description of the roles for TrendMicro and SSL software within the standard configuration

- Each MISA server requires InterScan WebProtect
- If an Exchange Server were being leveraged – which is not the case in this configuration – ScanMail would be used for that server
- A copy of ServerProtect is needed for every server
- Each BTRS server requires PortalProtect
- Each site requires an EnTrust SSL certificate



MISA Server

Internet

PIX

Switch
w/VLAN

Client Browser

MISA Server

TrendMicro
InterScan
Web Protect

Necessary Hardware

Optional Hardware

TrendMicro Software

Secure Socket Layer
Certificate (SSL)



APPENDIX 3 SOFTWARE LICENSE AGREEMENT



SOFTWARE LICENSE AGREEMENT

This Agreement dated as of March 17, 2003, ("**Effective Date**"), between Virtual Alert, Inc., a California corporation ("**Virtual Alert**") and the State of Michigan ("**Licensee**"), establishes the basis for a procurement relationship under which Virtual Alert licenses the Bio-Terrorism Readiness Suite software ("**Product**") described in the Purchase Order (defined below) issued under this Agreement.

1.0 Definitions:

"**Affiliates**" means entities that control, are controlled by, or are under common control with a party to this Agreement and that have signed a Purchase Order.

"**Agreement**" means this agreement and any relevant Purchase Order.

"**Contract**" means any document attached to or included in this Agreement which describes the Product, including any requirements or specifications, and is the only authorization for Virtual Alert to sell any product or to perform any work under this Agreement.

"**Derivative Work**" means a work that is based on an underlying work and that would be a copyright infringement if prepared without the authorization of the copyright owner of the underlying work.

"**Error Corrections**" means revisions that correct errors and deficiencies (collectively referred to as "Errors") in the Product.

"**Externals**" means any pictorial, graphic, or audiovisual works generated by execution of code and any programming interfaces, languages or protocols implemented in code to enable interaction with other computer programs or end users. Externals do not include the code that implements them.

"**Personnel**" means agents, employees, or contractors engaged by Licensee including persons that have been granted user authorization by Licensee.

"**Prices**" means the agreed upon payment and currency for Product and Services, including all applicable fees, professional services fees, royalty payments and taxes, as specified in the relevant Purchase Order.

"**Source Code**" means computer-programming code that may be displayed in a form readable and understandable by a programmer of ordinary skill.

2.0 Grant of License:

2.1 Right of Use. Virtual Alert will deliver to Licensee one complete copy of the Product described in the relevant Contract, which shall only be used for the purposes described herein. The product shall only be used by persons and for purposes within the State of Michigan. Virtual Alert will provide to Licensee, at no charge, Error Corrections for the Product beginning when Licensee accepts the Product and continuing for the Error Correction Warranty Period specified in the relevant Contract. The License hereby granted may not be transferred or sublicensed, but shall



extend to any department or subdivision of Licensee including persons granted user authorization by Licensee (collectively, "Affiliates"). Licensee shall be responsible for the compliance by each such Affiliate with the terms and provisions of this Agreement. Licensee shall not reverse engineer, reverse compile or disassemble the Product, or otherwise attempt to derive the Source Code to any software or technology licensed under this Agreement. The foregoing shall not apply to such activities conducted in the ordinary course of technical support of Licensee products such as may occur in the use of debugging tools.

Purchasing the Product is similar to purchasing many other "Common, Off-the-Shelf" software products. Licensee is purchasing a license for the right to use the product. The companies that designed and built the product and the related software platforms on which the software operates own the actual code behind the product and the Licensee will not receive Source Code, or the rights to the Source Code.

3.0 Term and Termination: Product acquired by Licensee on or after the Effective Date will be covered by this Agreement. This Agreement will remain in effect until terminated. Licensee may terminate a Purchase Order without cause within thirty (30) days of date of its receipt. Upon termination, Licensee shall return to Virtual Alert copies of all software received.

4.0 Pricing: Except for pre-approved expenses specified in the relevant contract, the Prices for Product specified in a contract and accepted by Licensee will be the only amount due to Virtual Alert in connection with the license. However, if Product is used for purposes other than those purposes described herein, or if the total amount of users exceeds the number of users licensed, additional license fees will be due.

5.0 Acceptance: The Product will be deemed accepted by Licensee and meeting all requirements unless it provides notice to Virtual Alert of non-conformity within thirty (30) days of date of its acceptance. For purposes of this section the State of Michigan agrees to accept or reject the product within 30 days from the date the software is activated for use by the State of Michigan. The parties agree that such acceptance shall not limit any of the remedies or rights otherwise provided to Licensee hereunder.

6.0 Representations and Warranties: Virtual Alert makes the following ongoing representations and warranties: (i) it has the right to enter into this Agreement and its performance of this Agreement will not violate the terms of any contract, obligation, law, regulation or ordinance to which it is or becomes subject; (ii) no claim, lien, or action exists or is threatened against Virtual Alert that would interfere with Licensee's rights under this Agreement; (iii) Product is safe for any use consistent with and will comply with the specifications and requirements in this Agreement; (iv) Product will be tested for, and does not contain, harmful code; (v) Product does not infringe any privacy, publicity, reputation or intellectual property right of a third party; and (vi) all authors have agreed not to assert their moral rights (personal rights associated with authorship of a work under applicable law) in the Product, to the extent permitted by law. **ONLY WRITTEN COMMUNICATIONS FROM VIRTUAL ALERT SHALL REPRESENT THE FUNCTIONAL AND TECHNICAL CAPABILITIES OF THE END PRODUCT. EXCEPT AS STATED IN THIS SECTION, VIRTUAL ALERT MAKES NO EXPRESS OR IMPLIED WARRANTIES, SUCH AS WARRANTIES OF PERFORMANCE, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.**

7.0 Intellectual Property



7.1 Right, Title and Interest. Contractor grants to the State non-exclusive, royalty-free, site-wide, irrevocable, transferable license to use the Software and related documentation according to the terms and conditions of this Contract. For the purposes of this license, "site-wide" includes any State of Michigan office, local hospitals and local public health department regardless of its physical location.

The State may modify the Software and may combine such with other programs or materials to form a Derivative Work. The State will own and hold all copyright, trademark, patent and other intellectual property rights in any Derivative Work, excluding any rights or interest in Software other than those granted in this Contract.

The State may copy each item of Software to multiple hard drives or networks. The State will make and maintain no more than one archival copy of each item of Software, and each copy will contain all legends and notices and will be subject to the same conditions and restrictions as the original. The State may also make copies of the Software in the course of routine backups of hard drive(s) for the purpose of recovery of hard drive contents.

7.2 Perfection of Copyrights: Upon request, Virtual Alert will provide to Licensee a "Certificate of Originality" or equivalent documentation to verify authorship of Product. Virtual Alert will be responsible for registration, maintenance and enforcement of copyrights for Products.

7.3 Names and Trademarks: Virtual Alert grants Licensee a nonexclusive, worldwide, perpetual, irrevocable, paid-up license to use the names and trademarks Virtual Alert uses to identify the Product for Licensee's marketing of the Product. If Virtual Alert objects to Licensee's improper use of Virtual Alert's names or trademarks, Licensee will take all reasonable steps necessary to resolve Virtual Alert's objections. Virtual Alert may reasonably monitor the quality of Product bearing its trademark under this license.

8.0 Indemnification

8.1 Remedies for Infringing Technology. In the event Virtual Alert reasonably believes that the use or distribution of any technology or Virtual Alert trademarks is likely to be enjoined, Virtual Alert may, at its option, either: (i) substitute functionally equivalent non-infringing technology; (ii) modify the infringing item so that it no longer infringes but remains functionally equivalent; or (iii) if none of the foregoing is feasible, Virtual Alert may take back such infringing item or items and terminate only that portion of the license associated with respect to such item or items, subject to a mutually satisfactory equitable reduction in the fees payable under this Agreement. STATE LICENSEE'S SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO CLAIMS OF INFRINGEMENT OF PROPRIETARY RIGHTS OF ANY KIND, AND ALL PURCHASE ORDER WARRANTIES OF NON-INFRINGEMENT, EXPRESS OR IMPLIED, ARE SPECIFICALLY DISCLAIMED AND EXCLUDED.



9.0 Confidentiality:

9.1 For the purposes of this Agreement, “Confidential Information” shall mean any information delivered by one party to another which the receiving party (“Receiving Party”) knows or has reason to know is considered confidential by disclosing party (“Disclosing Party”). Without limiting the foregoing, the technology, implementation methodologies, training methodologies, documentation, and if applicable, the Software Maintenance Agreement, shall be deemed Confidential Information, unless otherwise required by law. The Receiving Party agrees to take precautions to prevent any unauthorized disclosure or use of Confidential Information of the Disclosing Party consistent with precautions used to protect the Receiving Party’s own Confidential Information, but in no event less than reasonable care. Except as provided below, Licensee agrees to treat the Confidential Information as confidential and shall not disclose the Confidential Information to any person or entity without the Disclosing Party’s prior written consent. The Receiving Party may only disclose the Confidential Information to those who reasonably require access to such Confidential Information to perform obligations under this Agreement. The Receiving Party shall take all appropriate steps to ensure that its employees and contractors who are permitted access to the Confidential Information of the Disclosing Party agree to act in accordance with the obligations of confidentiality imposed by this Agreement. Should any party be faced with legal action to disclose Confidential Information under this Agreement, the Receiving Party shall promptly notify the Disclosing Party and upon the Disclosing Party’s request, shall reasonably cooperate with the Disclosing Party in contesting such disclosures. The obligations imposed by this Section shall survive any termination of this Agreement. The obligations set forth in this Section 9.0 shall not apply to any particular portion of any Confidential Information to the extent that: (i) now or subsequently becomes generally known or available through no act or omission of Receiving Party; (ii) was or is known at the time of receipt of same from Disclosing Party; (iii) is provided by the Disclosing Party to a third party without restriction on disclosure; (iv) is subsequently rightfully provided to Receiving Party by a third party without restriction on disclosure; or (v) is independently developed by Receiving Party and as can be demonstrated from Receiving Party’s business records and documentation, provided the person or persons developing same had not had access to the Confidential Information of the Disclosing Party prior to such independent development.

10.0 Liability: EXCEPT FOR LIABILITY FOR BREACH OF SECTION 9 (CONFIDENTIALITY) AND EXCEPT AS SPECIFICALLY PROVIDED IN SECTION 8 (INDEMNIFICATION): (A) NEITHER PARTY SHALL HAVE ANY LIABILITY FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL OR PUNITIVE DAMAGES OF ANY KIND OR FOR LOSS OF REVENUE OR LOSS OF BUSINESS ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, REGARDLESS OF THE FORM OF THE ACTION, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT PRODUCT LIABILITY OR OTHERWISE, EVEN IF ANY REPRESENTATIVE OF A PARTY HERETO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES; AND (B) **IN NO EVENT SHALL VIRTUAL ALERT’S LIABILITY UNDER THIS AGREEMENT EXCEED THE TOTAL CONTRACT AMOUNT.**



- 11.0 Recordkeeping and Audit Rights:** Virtual Alert will maintain (and provide to Licensee upon request) relevant accounting records to support invoices under this Agreement and proof of required permits and professional licenses, for two (2) years following completion or termination of the relevant Purchase Order. All accounting records will be maintained in accordance with generally accepted accounting principles.

Virtual Alert may, in its discretion and at any time, audit the number of users by Licensee and its Affiliates to ensure compliance with this Agreement and Purchase Order.

- 12.0 General:** This Agreement may only be amended by a writing specifically referencing this Agreement which has been signed by authorized representatives of the parties. Virtual Alert may assign this Agreement to any person to whom it transfers all or substantially all of its rights in the technology. Except as provided in the preceding sentence, neither party may assign, voluntarily, by operation of law, or otherwise, any rights or delegate any duties under this Agreement (other than the right to receive payments) without the other party's prior written consent. Any attempt to do so without that consent will be void. This Agreement will bind and inure to the benefit of the parties and their representative successors and permitted assigns. This Agreement will be governed by and construed in accordance with the laws of the United States and the State of Michigan as applied to agreements entered into and to be performed entirely within Michigan between Michigan residents. The parties agree that the United Nations Convention on Contracts for the International Sale of Goods (1980) is specifically excluded from application to this Agreement. This Agreement may be signed in one or more counterparts, each of which will be deemed to be an original and all of which when taken together will constitute the same agreement. Any copy of this Agreement made by reliable means is considered an original. Affiliates will acknowledge acceptance of the terms and conditions of this Agreement through the signing of a Purchase Order before conducting any transaction under this Agreement

- 13.0 Conflict in the Documents.** If any provision(s) of this Agreement conflict(s) with the terms of the State of Michigan Contractual Service Terms and Conditions attached hereto, then the State of Michigan Contractual Service Terms and Conditions shall be controlling

- 14.0 Software License Agreement.** Source Code License and Use Agreement (Released from Escrow)

14.1 Licensee Restrictions

- 14.1.1** Licensee shall reproduce and include any and all copyright notices and proprietary rights legends, as such notices and legends appear in the original Software, on any copies of the Software, including any Permitted Modifications and any Run-Time Modules.
- 14.1.2** The Software Source Code and all Permitted Modifications in Source Code shall be handled, used and stored, solely at an Authorized Site. Although the Software Source Code may be used either from a single machine or a server, there shall be no external network access to such code (i.e., by any computers or terminals not located at the Authorized Site).



14.1.3 Licensee shall not disclose, sell, sublicense, license, transfer, market, distribute, rent, lease, timeshare, loan or otherwise make available the Software Source Code or any Permitted Modifications in Source Code to any third party unless such third party is under contract with the Licensee to repair the Product and has executed and delivered to Virtual Alert a Non-Disclosure and Non-Circumvention Agreement acceptable to Virtual Alert.

14.1.4 Access to the Software Source Code shall be limited to five (5) employees of Licensee who (i) require access to the Software Source Code for the purposes authorized by this Agreement, and (ii) have signed an employee or other agreement in which such employee agrees to protect third party confidential information with terms no less stringent than those set forth herein. Licensee agrees that any breach by any employee of its obligations under such confidentiality agreements shall also constitute a breach by Licensee hereunder. For the purposes of this Agreement, the definition of "employee" shall be as defined for purposes of the U.S. Copyright Act and expressly excludes independent contractors. Licensee shall maintain and, upon Virtual Alert's reasonable request, provide to Virtual Alert, the names of all employees who have had access to the Software Source Code.

14.1.5 Licensee shall use its best efforts to protect the Software Source Code from unauthorized access, reproduction, disclosure or use. In the event Licensee becomes aware of any unauthorized use or disclosure of the Software Source Code, Licensee shall notify Virtual Alert immediately in writing and shall give full cooperation, at Licensee's expense, to minimize the effects of such unauthorized use or disclosure.

15 CONFIDENTIAL INFORMATION. Licensee shall not use or disclose any Confidential Information, except as expressly authorized by this Agreement, and shall protect all such Confidential Information using the same degree of care which Licensee uses with respect to its own proprietary information, but in no event with safeguards less than a reasonably prudent business would exercise under similar circumstances. Licensee's obligations regarding the protection of Confidential Information shall survive any expiration or termination of the Agreement. Licensee shall take prompt and appropriate action to prevent unauthorized use or disclosure of the Confidential Information.

16 OWNERSHIP. Licensee shall have an obligation to provide or disclose to Virtual Alert or its successors or assigns any Permitted Modifications. Virtual Alert and its successor and assigns shall retain exclusive ownership of all worldwide Intellectual Property Rights in and to the Software and Source Code. Licensee hereby assigns to Virtual Alert any such rights Licensee may have or obtain in and to the foregoing. All rights in and to the Software not expressly granted to Licensee in this Agreement are expressly reserved for Virtual Alert.

17 DELIVERY; RECORDS AND AUDITS.

17.1 Delivery. Delivery to Licensee shall be controlled by the Software Source Code Escrow Agreement executed by the Parties to which the Agreement is an exhibit. Such Software shall be deemed irrevocably accepted upon release by Escrow Agent.



17.2 Records, Distribution Reports. Licensee shall maintain complete, current and accurate records documenting all Run-Time Module copies made and distributed by or for Licensee in Target Applications, the location of the Software (in all forms) in Licensee's, its distributors' and its manufacturers' possession, and the names of all persons who have had access to the Software Source Code. Within thirty (30) days of the end of each calendar year or upon demand by Virtual Alert which shall not occur more frequently than once per calendar quarter. Licensee shall submit to Virtual Alert or its successors or assigns a written report which shall set forth the number of Target Applications distributed by Licensee and such other information as Virtual Alert may reasonably request (herein, the "Target Report"). If no Target Applications were distributed within a given quarter, Licensee shall provide to Virtual Alert a statement so certifying. Except where Licensee is reporting Target Applications for which Licensee has pre-paid Virtual Alert its applicable per copy license fees, Licensee shall enclose with the Target Report, Virtual Alert's stipulated per copy license fee for the activity reported which exceed the number or original licenses purchased under the Purchase Agreement

17.3 Audits. To ensure compliance with the terms of this Agreement and the payment of any additional license fees due hereunder, Virtual Alert or its authorized designee shall have the right to inspect and audit all the records and distribution reports and all relevant books and records of Licensee, to obtain true and correct photocopies of such records, and to obtain such other information as necessary to determine Licensee's compliance with this Agreement. At Virtual Alert's request, Licensee shall provide reasonable assistance to Virtual Alert in conducting such inspection and audit. Such audit shall be conducted during regular business hours at Licensee's offices and in such a manner as not to interfere unreasonably with Licensee's normal business activities. In no event shall such audits be conducted hereunder more frequently than once every six (6) months. If such audit should disclose any underpayment of royalty fees, Licensee shall promptly pay Virtual Alert such underpaid amount. If the audit reveals that Licensee has underpaid Virtual Alert by five percent (5%) or more of the amount paid, then Licensee shall immediately reimburse Virtual Alert for Virtual Alert's expenses associated with such audit.

18 TERM AND TERMINATION. This Agreement shall commence upon the Effective Date and continue until terminated as set forth in this Agreement. This Agreement will immediately terminate upon Licensee's breach of this Agreement, unless such breach is curable and is cured by Licensee within ten (10) days after notice of such breach is provided by Virtual Alert. Upon termination, Licensee agrees: (i) not to use the Software for any purpose whatsoever; (ii) to destroy the Software and any copy then in Licensee's possession; and (iii) to certify to Virtual Alert that such destruction has taken place. Upon termination Virtual Alert may repossess all copies of the Software then in Licensee's possession or control. Termination of this Agreement shall also terminate any End User sublicenses previously granted by Licensee. These remedies shall be cumulative and in addition to any other remedies available to Virtual Alert.



19 KEYS AND ACCESS. Virtual Alert agrees to provide to Licensee those Software keys which are reasonably necessary to permit Licensee to gain access to the Software contained on media released by Escrow Holder if such keys are not released with the Source Code or for some reason are incorrect. All such keys shall be considered the Confidential Information of Virtual Alert. Notwithstanding anything to the contrary in this Agreement, Licensee hereby acknowledges that Licensee shall have no right or license to any software released by Escrow Holder on media as provided above which software is not properly licensed pursuant to a license agreement between the parties, that any such software is included therein solely as a matter of administrative convenience, and Licensee further agrees not to attempt to gain access to, or permit any third party to attempt to gain access to, such software. Licensee shall not disclose the Software keys to any third party.

20 WARRANTY.

20.1 Limited Warranty. Virtual Alert warrants that the media on which the Software is delivered will be free from defects in materials or workmanship on the date Virtual Alert ships the media to Escrow Holder. If the media on which Software is delivered proves to be defective, Virtual Alert will replace such media and as Licensee's sole remedy. When the Source Code is released by Escrow Agent to Licensee, Licensee assumes full responsibility for: (i) the application of the Source Code for the purpose which Licensee sought release from the Escrow Holder; (ii) verifying the results obtained from the use of the Source Code; and (iii) taking appropriate measures to prevent loss of data. Virtual Alert does not warrant that the operation of the Software will meet Licensee's requirements or that Licensee will be able to achieve any particular results from use or modification of the Software or that the Software will operate free from error.

20.2 Warranty Disclaimer. EXCEPT AS EXPRESSLY SET FORTH IN SECTION 10, VIRTUAL ALERT AND ITS SUCCESSORS AND ASSIGNS DISCLAIM ALL WARRANTIES, EXPRESS, IMPLIED AND STATUTORY INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY VIRTUAL ALERT, ITS DEALERS, DISTRIBUTORS, AGENTS OR EMPLOYEES SHALL IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY.

21 SUPPORT. The release of the Source Code by Escrow Holder does not imply and Virtual Alert does not provide support, installation or training for any Software released by Escrow Holder. Installation and training services, to the extent offered by Virtual Alert, may be separately purchased at Virtual Alert's then-current rates. Notwithstanding the foregoing, Virtual Alert is not obligated to support the Software running on an operating system not provided by Virtual Alert. Licensee may request additional information on Virtual Alert's support offerings from a Virtual Alert.



22 INDEMNIFICATION.

Virtual Alert's Indemnity. Virtual Alert will defend any suit brought against Licensee and will pay all damages finally awarded in such suit insofar as such suit is based on a claim that the Source Code as provided to the Escrow Holder infringes a previously issued United States patent or copyright, provided that Virtual Alert is notified promptly of such claim and at its expense is given full and complete authority (including settlement authority), information and assistance by Licensee for such defense. This obligation shall not apply to infringement actions or claims to the extent that such actions or claims are based on or result from: (i) modifications made to the Software by a party other than Virtual Alert; and (ii) the combination of the Software with items not supplied by Virtual Alert. THIS SECTION STATES LICENSEE'S EXCLUSIVE REMEDY AND VIRTUAL ALERT'S ENTIRE LIABILITY FOR ANY CLAIM OF INFRINGEMENT. .

IN WITNESS WHEREOF, the parties have caused this Agreement to be duly executed and delivered on the day and year first above written.

ACCEPTED AND AGREED TO:

ACCEPTED AND AGREED TO:

By: _____
Signature Date

By: _____
Signature Date

Printed Name

Virtual Alert, Inc.



APPENDIX 4

EQUIPMENT LOCATION AND SERVICES AGREEMENT



EQUIPMENT LOCATION AND SERVICES AGREEMENT

This Equipment Location and Services Agreement (“Agreement”) is made as of the Seventeenth day of March, 2003, between Virtual Alert, Inc., a California corporation (“Virtual Alert”), and the State of Michigan (“MICHIGAN”), for location of certain equipment in a facility contracted or maintained by Virtual Alert (the “Site”), and for purchase of certain related services, as defined herein.

1. LICENSE.

(a) GRANT. MICHIGAN is given a non-exclusive license (“License”) to use identified Virtual Alert contracted or maintained broadband facilities for authorized connections of its equipment at the Site, in a place determined or mutually agreed between Virtual Alert and MICHIGAN on the terms and conditions stated herein. Any area occupied by MICHIGAN’s equipment is described as the “Space”.

MICHIGAN understands that Virtual Alert subleases Sites from companies that own and maintain secure, co-location or master hosting facilities and Virtual Alert has an agreement with those master facility operators to provide the services to Virtual Alert and MICHIGAN under terms similar to this Agreement. Virtual Alert is entirely responsible to the facility operator and agrees to hold MICHIGAN harmless and indemnify MICHIGAN against any claim by any master facility provider so long as MICHIGAN is in compliance with the terms of this Agreement. MICHIGAN will be provided with the opportunity to inspect the Site prior to entering into this Agreement.

(b) ADDITIONAL SERVICES. If Virtual Alert is providing MICHIGAN with services (“Services”) in addition to the License, such Services are listed on Schedule 1, and MICHIGAN agrees to pay for the additional Services as provided in this Agreement.

(c) ADDITIONAL SPACE. Any additional space, connections or Services sought by MICHIGAN at the Site after the date hereof shall be covered by a separate written Schedule, numbered in sequence, dated, and signed by each party, that references this Agreement, and that identifies the new items, the pricing, and any new or additional terms and conditions. This Agreement will control the provision of all such additional items to the extent that new or additional terms and conditions are not stated therein.

(d) LIMITS ON GRANT. All rights or privileges of MICHIGAN outlined in this Agreement and related to the Site are nonexclusive. MICHIGAN’s use of the Space shall not interfere with the use or occupancy of the Site by Virtual Alert, its other customers or any other user of the Site. Virtual Alert reserves all rights and privileges related to the Site not specifically granted to MICHIGAN herein, including the right to access and use any part of the Site, and to establish regulations in connection with the Site use by any person.



(e) MODIFICATION OF LOCATION / TERMS AND CONDITIONS. Virtual Alert reserves the right to relocate MICHIGAN within the Site and/or to modify the terms (excluding contracted pricing) and conditions under which connections are provided, on thirty (30) days' written notice to MICHIGAN. Any relocation will be at no cost to MICHIGAN. If the change causes MICHIGAN to be substantially unable to operate in the manner in which it was operating directly prior to the change, MICHIGAN reserves the right to charge Virtual Alert for all actual damages incurred or at its option to cancel this contract on ten (10) days' written notice subject to payment for space, connections and Services through the time MICHIGAN exits the Site.

2. TERM.

(a) INITIAL TERM. The initial term ("Term") of this Agreement is through September 30, 2003, commencing on the first business day that MICHIGAN is connected within the Space by Virtual Alert.

If Virtual Alert is unable to make the Site or Space or related connections available to MICHIGAN within twenty (20) days of any Virtual Alert-identified delivery date, this License shall not be affected, but MICHIGAN shall be relieved of its obligation to pay for any Space and connections not provided until it is tendered. If a failure to tender the Site or Space or connections extends for more than thirty (30) days, and no reasonably acceptable alternative space or connections are made available to MICHIGAN, MICHIGAN may cancel this Agreement without further obligation under this Agreement.

(b) TERMINATION NOTICE FROM MICHIGAN. If MICHIGAN elects to terminate this License at the end of the Term, it shall provide ten (10) days written notice of termination to Virtual Alert.

(c) MINIMUM FEES. MICHIGAN and Virtual Alert have agreed that MICHIGAN must purchase at least three (3) months of Services from Virtual Alert, at the rates set forth in Schedule 1, and that this must be paid upfront.

(d) TERMINATION FOR NON-PAYMENT. Virtual Alert, Inc. is responsible to pay any or all fees due to the Subcontractors under this agreement. In the event that full payment of any or all fees due to the Subcontractors under this agreement have not been received within 30 days of payment due date, the Subcontractors will notify ALL parties regarding non-payment or potential cancellation of services. If the delinquent fees are not received within 30 days of the delinquent notification, the Subcontractors under this agreement shall have the right to terminate this agreement.

3. USE.

(a) MICHIGAN USE AND LIMITS. Space, connections and Services are provided for MICHIGAN's equipment which is maintained for MICHIGAN by Virtual Alert. MICHIGAN may not provide service provider interconnections at any place within the Site independent of Virtual Alert and may not directly interconnect its equipment in the Space



to the facility of any other provider or MICHIGAN of Virtual Alert on site without the prior written consent of Virtual Alert.

As part of this Agreement, Virtual Alert shall secure and maintain MICHIGAN's equipment to be located at the Site and shall ensure that neither it nor any person accessing the site on behalf of MICHIGAN damages any part of the Site or any equipment located in or around the Site. MICHIGAN shall be permitted on the site with advance notice to Virtual Alert to inspect the equipment and services provide but shall not perform or permit any violation of laws, rules, regulations or ordinances of any governmental agency with respect to the Site, and MICHIGAN shall not act in any way that is a nuisance to Virtual Alert or to other users of the Site. If MICHIGAN does visit the site, MICHIGAN shall not act in any manner that interferes with communications or computer operations at the Site in any manner, including interference through radio spectrum use, electromagnetic fields or any form of radiation. MICHIGAN shall not use the Site for any purpose that would invalidate or increase the premium on insurance related to the Site. MICHIGAN will make clear to its employees and agents who visit the site that alcoholic beverages, controlled dangerous substances and weapons or other dangerous instrumentalities are prohibited at the Site at all times.

(b) NO ENCUMBRANCES. MICHIGAN shall not assign, mortgage, sublease, encumber or otherwise transfer this Agreement, the License or any rights of MICHIGAN under this Agreement. Any attempt or action by MICHIGAN to do so shall be void.

(c) BREACH AND REMOVAL OF EQUIPMENT ON TERMINATION OF LICENSE. MICHIGAN shall not remove any of its equipment on or before September 30, 2003 upon which this Agreement ends. Virtual Alert may remove any such equipment, disconnect such equipment and store it at the expense of MICHIGAN if MICHIGAN is in violation of this Agreement. In the event of such breach by MICHIGAN, Virtual Alert will notify MICHIGAN to take possession of its equipment within thirty (30) days thereafter; Virtual Alert may deem such to have been abandoned. Thereafter, Virtual Alert may, without further notice, remove, sell, abandon or otherwise dispose of the equipment without incurring liability to MICHIGAN, and may apply any sums recovered to any amounts due Virtual Alert from MICHIGAN.

4. FEES AND BILLING.

(a) BASIC FEES AND CHARGES. MICHIGAN agrees to pay fees and charges as set out in Schedule 1, or as otherwise provided for in this Agreement.

(b) MICHIGAN-REQUESTED CHANGES. At any time after execution of this Agreement, MICHIGAN may request upgrades, changes or improvements to accommodate the level of services of its equipment at the Site. Virtual Alert will consider all such requests and advise MICHIGAN whether such changes or improvements can be made and the costs. If MICHIGAN and Virtual Alert agree upon such changes and improvements and the related price, the parties shall execute a separate Schedule in the same manner as provided for in Section 1(d). All changes



and improvements will require the approval of Virtual Alert and are subject to the approval of the master facility operator if the Site is located in a facility other than one owned by Virtual Alert.

5. PAYMENT, PAYMENT DISPUTES, LATE FEES AND TAXES.

(a) **BASIC PAYMENT OBLIGATION.** All monthly recurring fees and charges, shall be payable by MICHIGAN in advance on or before the first day of each calendar month. One time and non-recurring charges and fees are due and payable in full upon invoice. Charges for burstable bandwidth or other measured or usage based charges will be billed in arrears. Payments are due without setoff, abatement or deduction of any kind. Invoices become past due thirty (30) days after receipt, which is deemed to be five (5) days after mailing by or on behalf of Virtual Alert. Adjustments made to space, connections or Services will be prorated on the basis of number of days it was provided or available in the billing month. Any invoices will be sent to the most recent address on file with Virtual Alert.

(b) **PAYMENT DISPUTES, INTERIM PAYMENT AND ESCALATION.** If MICHIGAN disputes any charges or fees contained in an invoice, MICHIGAN shall notify Virtual Alert in writing of the dispute not later than the date that the invoice is payable. MICHIGAN shall pay all undisputed amounts in full (including amounts that would be due at any different rate(s) claimed applicable by MICHIGAN) by the due date. Any claim shall be *bona fide* and supported by an explanation of the basis for the dispute. Failure to timely submit a dispute notification shall waives the right to dispute the invoice, and the invoice shall become final and conclusive. If the dispute is resolved in MICHIGAN's favor, the amount so resolved will be refunded or credited to MICHIGAN, including any related late fee or interest.

6. SECURITY DEPOSIT AND OTHER CHARGES.

(a) **SPECIAL INSTALLATIONS.** MICHIGAN is responsible for coordinating in advance with Virtual Alert for the delivery of any MICHIGAN equipment, including cabinets, racks, and overhead cable ladders permitted by Virtual Alert in addition to what is already at the Site. MICHIGAN is responsible for ordering from Virtual Alert any caging, pre-wiring, earthquake mounting/bracing and other installation Services. All such additional installation Services shall be made available at Virtual Alert's prevailing rate(s) and subject to availability by any master facility operator that Virtual Alert contracts for the Site or Space.

7. CANCELLATION.

Cancellation by the State shall be governed by the State of Michigan Contractual Service Terms and Conditions as indicated in I-T section of the contract.

8. MAINTENANCE.



(a) MICHIGAN OBLIGATION. Unless otherwise provided in a Schedule to this Agreement, maintenance of all equipment of MICHIGAN shall be performed by Virtual Alert according to the terms of the agreement between the Parties on a mutually agreeable time schedule.

(b) LIMITATIONS ON VIRTUAL ALERT'S OBLIGATION. Virtual Alert shall be responsible for maintenance of the Site, except for defects or failures caused by MICHIGAN. The Site shall be maintained in compliance with all applicable fire and safety code requirements. Virtual Alert shall be responsible for the repair; operation or maintenance of the equipment supplied by MICHIGAN provided it is installed by Virtual Alert. Virtual Alert is not responsible for the transmission or reception of signals at the Site, or for the quality of, or any problems with any transmission experienced by MICHIGAN or any user of MICHIGAN's equipment or services. The furnishing of any Service under this Agreement is subject to the availability on a continuing basis of all necessary underlying facilities and services, as well as facilities Virtual Alert may obtain from other master facility operators or carriers with which Virtual Alert has master agreements. Virtual Alert does not undertake to transmit messages for MICHIGAN or any agent or employee of MICHIGAN, and shall not be liable for errors in transmission or for the failure of MICHIGAN or any other person to establish connections

(c) SCHEDULED AND UNSCHEDULED OUTAGES AND MAINTENANCE. Virtual Alert will attempt to provide MICHIGAN with reasonable advance notification (not less than three (3) business days) of any scheduled AC or DC power maintenance work, and any related activity at the Site that is reasonably be expected to impact the power availability or Services of MICHIGAN. Virtual Alert will advise MICHIGAN immediately of any emergency or unscheduled activity that would reasonably be expected to impact the power availability or telecommunications services of MICHIGAN. MICHIGAN agrees that Virtual Alert may reduce, pro rata or according to any formula or arrangement permitted by law, heat, light, power, or water as required by applicable governmental or quasi-governmental conservation or similar programs.

9. ACCESS / ACCESS CONDITIONS.

(a) ESCORTED ACCESS. MICHIGAN may procure escorted access to the Site on a prescheduled basis by contact with Virtual Alert at least 10 days prior to such access, unless on an emergency basis then Virtual Alert will make every effort to accommodate the request for access. If such access is requested MICHIGAN shall provide to Virtual Alert a list of all persons who are to be afforded access to the Site. Virtual Alert is under no obligation to allow entry to any person not so identified, and may restrict access by any person who violates any rules or conditions related to the Site. Entry for the purpose of installation or removal of equipment shall be done only with a Virtual Alert escort.

Any installation or removal of equipment may be performed only in the presence of an authorized Virtual Alert technician. If the time required for installation or removal is greater than the standard interval identified by Virtual Alert, MICHIGAN may be assessed a time charge for the time commitment required. Removal of equipment shall not be



permitted where MICHIGAN is in default on its payment obligations under this Agreement.

(b) WORK RULES AND REGULATIONS FOR OCCUPANCY AND USE. From time to time, Virtual Alert will advise MICHIGAN of any work rules and regulations generally applicable to the Site, and any new or revised rules and regulations. MICHIGAN agrees to comply with such reasonable rules and regulations and to cause its employees, representatives, agents, invitees, and contractors ("Permittees") to comply with all such rules and regulations.

10. BREACH AND TERMINATION.

(a) MICHIGAN BREACH. The following circumstances constitute a breach of this Agreement by MICHIGAN: (i) MICHIGAN fails to pay any outstanding unpaid fees or charges within forty-five (45) days of the due date, except amounts for which a timely raised dispute is pending and unresolved; (ii) MICHIGAN fails to comply with any other material term or condition of this Agreement or to cure such non-compliance within thirty (30) days after written notice; or (iii) MICHIGAN fails to comply with any other term or condition of this Agreement or to cure such non-compliance within forty-five (45) days after written notice. A material breach of any other agreement between Virtual Alert and MICHIGAN (or any MICHIGAN affiliate) in connection with the Site shall constitute a material breach of this Agreement.

(b) REMEDIES FOR MICHIGAN BREACH. If MICHIGAN is in breach, Virtual Alert may, within thirty (30) days after written notice, at its option, take any or all of the following actions: (i) cancel this Agreement and the services hereunder, or any portion thereof; (ii) temporarily suspend Services and connections or otherwise block use by MICHIGAN of the Site; (iii) decline to accept or to process any orders from MICHIGAN; (iv) commence action to collect all sums then due or that subsequently become due; (v) cancel and make the Space used by MICHIGAN available to other interested persons; (vi) cancel and accelerate and collect any termination charges, including termination charges in connection with any term, volume or other purchase commitment; and (vii) take any additional steps permitted by law. If Services are discontinued, terminated or suspended, restoration or resumption of service shall occur or be denied in the sole discretion of Virtual Alert and Virtual Alert may require payment of a resumption fee prior to restoring service. If the Service is restored, it shall not be deemed a waiver of MICHIGAN's breach.

(c) SURRENDER OF SPACE. If Virtual Alert terminates this Agreement for breach by MICHIGAN, MICHIGAN shall terminate use of the Space and remove its equipment from the Site. Within 30 days written notice of termination Virtual Alert may terminate MICHIGAN's use and/or occupancy and remove all MICHIGAN equipment from the Site, shipping it to MICHIGAN or storing it at MICHIGAN's expense.



(d) **VIRTUAL ALERT BREACH.** If Virtual Alert fails to comply with any material term or condition of this Agreement, and fails to cure such failure within thirty (30) days after written notice; or fails to comply with any other term or condition of this Agreement within forty-five (45) days after written notice it shall be in breach. In the event of Virtual Alert breach, MICHIGAN may: (i) cancel this Agreement and any related agreements; (ii) seek injunctive or other equitable relief to the extent merited.

(e) **LITIGATION COSTS.** Each party shall bear their own attorneys' fees and court costs in any dispute.

(f) **OTHER VIRTUAL ALERT TERMINATION RIGHT.** The License and this Agreement are immediately terminable by Virtual Alert if Virtual Alert's authority to provide the Space and any Services at the Site terminates. If Virtual Alert so terminates the License, Virtual Alert shall give to MICHIGAN written notice of such termination within thirty (30) days, and the termination shall become effective as stated in the notice. The parties shall establish a time, not to exceed thirty (30) days, for MICHIGAN to remove its equipment. MICHIGAN shall pay for Space and connections and Services through the time of termination. If MICHIGAN does not timely remove its equipment, Virtual Alert may remove such equipment and store it for MICHIGAN at MICHIGAN's expense.

11. INSURANCE. Insurance provisions shall be governed by the State of Michigan contractual service terms and conditions as indicated in I-R section of the contract.

12. DAMAGE TO AREA USED BY MICHIGAN.

(a) **FIRE OR CASUALTY – LEASE TERMINATION OR NO REBUILDING.** If the Site is damaged by fire or other casualty, or by a natural occurrence, or by other accident, destructive event or action, and such damage is reasonably expected to impact the use of the Site by MICHIGAN, Virtual Alert shall give prompt written notice to MICHIGAN.

If Virtual Alert (or its landlord or master facility operator) exercises an option to terminate use of the Site, or if Virtual Alert (or its landlord or master facility operator) decides not to rebuild that portion of the Site in which MICHIGAN is located, this Agreement shall terminate as of the date of such exercise or decision as to the Site or the affected area(s), and the License and this Agreement shall be terminated.

MICHIGAN shall be afforded a reasonable time, not to exceed thirty (30) days, to remove and/or relocate any facilities and equipment. If MICHIGAN does not remove its equipment within such period, Virtual Alert may remove such equipment and store it at MICHIGAN's expense. No charges or fees shall be payable for the Space for periods subsequent to the termination of the License and this Agreement. The Contractor shall be required to relocate the site while they rebuild.



If MICHIGAN is caused to be unable to use the Space for thirty (30) after such fire or other casualty, then unless Virtual Alert moves MICHIGAN within such time and at no cost to MICHIGAN to an alternative space from which MICHIGAN can operate, MICHIGAN may terminate this Agreement without further obligation on five (5) days written notice to Virtual Alert, except for amounts due through the commencement of the five (5) business day period.

(b) REPAIR. If neither the landlord, or master facility operator of the Site nor Virtual Alert exercises the right to terminate or the right not to rebuild, then the area in which MICHIGAN is located shall be repaired within a reasonable time to a condition from which MICHIGAN can operate. In the event that such repairs are not completed within a reasonable time (not to exceed ninety (90) days), MICHIGAN may elect to terminate this Agreement on ten (10) days' written notice. The contractor shall be required to relocate the site while they rebuild.

(c) TEMPORARY ABATEMENT OF CHARGES. If, through no fault of MICHIGAN, the Site is rendered unusable due to fire or casualty, but subsequently repaired, fees and charges for the Space shall abate proportionately while MICHIGAN is unable to use the Space, for the period from the date of such damage to the date when such damage shall have been repaired and MICHIGAN's use is restored.

13. INDEMNIFICATION; LIMITATION OF LIABILITY; NO WARRANTIES.

(a) LIMITATION OF LIABILITY. MICHIGAN agrees that Virtual Alert shall have no liability to MICHIGAN or its Permittees who may enter the Site, or to others who suffer death, injury or damage if caused by MICHIGAN or a MICHIGAN Permittee. This Agreement does not purport to limit liability where liability cannot be limited as a matter of law. To the extent that liability cannot be disclaimed, Virtual Alert's entire liability hereunder for any claims shall not exceed the total amount of the contract. This limitation shall survive expiration or termination of this Agreement.

(b) NO WARRANTY / DISCLAIMER / DAMAGES LIMITATION. MICHIGAN recognizes that Virtual Alert is itself a lessee of the Site from a third party, and that the Site may be located on land formerly part of a government facility. MICHIGAN agrees that Virtual Alert specifically disclaims any promise, condition, representation or warranty, including any implied promise, condition, representation or warranty that the Site is in compliance with environmental laws, rules, regulations or other requirements, whether Federal, state, local or otherwise, and MICHIGAN agrees that it is accepting and using the Site "AS IS".

THE PARTIES AGREE THAT THERE ARE NO EXPRESS OR IMPLIED WARRANTIES GIVEN BY EITHER PARTY IN CONNECTION WITH THE PROVISION OF ANY SPACE, CONNECTIONS, EQUIPMENT OR SERVICES AT THE SITE, AND ANY AND ALL SUCH WARRANTIES, EXPRESS OR IMPLIED, ARE SPECIFICALLY DISCLAIMED.



IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY LOST REVENUE OR PROFITS (OTHER THAN FEES AND CHARGES PAYABLE FOR SPACE, CONNECTIONS OR SERVICES), OR FOR DAMAGES FOR LOST DATA, FAILURES OF CONNECTIONS OR BUSINESS INTERRUPTION, OR FOR ANY SPECIAL, CONSEQUENTIAL OR INDIRECT DAMAGES THAT ARE IN ANY WAY RELATED TO THIS AGREEMENT, EVEN IF SUCH LOSS OR DAMAGES WERE FORESEEABLE AND EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES.

14. CONFIDENTIALITY OF VIRTUAL ALERT INFORMATION. Unless otherwise required by law, MICHIGAN agrees that if it is afforded access to Virtual Alert facilities for installation, repairs, maintenance, administration or other purpose, MICHIGAN will not copy, record or remove any Virtual Alert material, data or other information of any kind, including information about the facilities, and will not take any action that reasonably could cause the disclosure or availability of any Virtual Alert material, information or data to any person who is not affiliated with Virtual Alert and authorized to have access to such information.

15. RESPONSIBILITIES REGARDING ACCEPTABLE USE.

(a) **COMPLIANCE WITH LAW.** MICHIGAN shall assure that its actions and the actions of its staff when visiting the Site will not be defamatory in nature, nor shall it infringe on any copyright, trademark or patent, or violate any trade secret or other intellectual property right of any third party or any federal, state, or local law, regulation or ordinance, including those pertaining to obscenity, that are applicable in any geographical area where the content generated by such use can be viewed or retrieved.

(b) **ACCEPTABLE USE POLICY.** MICHIGAN shall, at all times while using the Services abide by Virtual Alert's or the master facility operators Acceptable Use Policy as established by Virtual Alert or the master facility operator and modified from time to time. Each Authorized User may be required to complete a registration, update information as necessary to maintain accuracy of user records over the period of the Agreement, use the Services only for lawful and appropriate purposes, participate in the password assignment process, and maintain his/her password in strict confidence.

(c) **ACTIONS - VIOLATIONS OF LAW.** Upon thirty (30) days written notice Virtual Alert reserves the right to suspend or terminate Services provided to MICHIGAN at any time for any activity by MICHIGAN or MICHIGAN's users that in Virtual Alert's reasonable discretion constitutes a violation of applicable federal or state law or regulation until such activity ceases or is appropriately modified. MICHIGAN acknowledges that suspension will result in the complete cessation of all Internet access to and from the MICHIGAN.



Virtual Alert shall have no liability or responsibility for the content of any communications transmitted by MICHIGAN or any other party using the Services, or any other person. MICHIGAN shall provide a contact name to Virtual Alert to assist Virtual Alert in connection with compliance with the Digital Millennium Copyright Act.

16. Reserved.

17. FORCE MAJEURE. Neither party shall be liable for any failure of performance of equipment or Services due to causes beyond such party's reasonable control, including but not limited to: acts of God, fire, flood or other catastrophes, any law, regulation, direction, action, or request of any governmental entity or agency, or any civil or military authority, national emergencies, terrorism or similar destructive acts, third party fiber or cable cuts, insurrections, riots, wars, unavailability of rights-of-way or materials, strikes, lock-outs, work stoppages, carrier bankruptcy or default, utility power crisis, or labor difficulties (collectively, a "force majeure").

18. ASSIGNMENT. MICHIGAN may not transfer or assign this Agreement or any rights or privileges under it without the express prior written consent of Virtual Alert. Any attempt to transfer or assign in violation of this provision shall be void. Virtual Alert may condition approval of any assignment to assure that it will not be prejudiced or compromised, and if the assignee agrees in writing to be bound by the provisions of this Agreement. Unless Virtual Alert otherwise agrees in writing, upon an assignment MICHIGAN shall remain liable for all charges due and payable under this Agreement and any related agreement.

19. NOTICES. All notices, consents and other communications required or permitted hereunder shall be in writing and shall be personally served, mailed or delivered as follows (or to such additional or other persons at such other address or addresses as may be designated by notice of the appropriate party).

If to Virtual Alert:

Virtual Alert, Inc.
Box 2985
La Jolla, California 92038
Attn: Chris Popov

If to MICHIGAN:

William Colville
Health Alert Network Coordinator
Michigan Department of Community Health
3423 No. Martin Luther King Blvd.
Lansing MI 48909



Mailed communications shall be sent by certified or registered mail, postage prepaid or by a generally recognized overnight delivery carrier such as USPS Overnight Mail, FedEx or UPS. Such communications shall be deemed effective on the date of delivery identified by the carrier to the appropriate party. Facsimile delivery is effective only upon confirmation by the recipient.

20. CONFLICT IN THE DOCUMENTS.

If any provision(s) of this agreement conflict(s) with the terms of the State of Michigan Contractual Service Terms and Conditions attached hereto, then the State of Michigan Contractual Service Terms and Conditions shall be controlling.

21. GENERAL AND MISCELLANEOUS PROVISIONS.

(a) ENTIRE AGREEMENT; MODIFICATION OF AGREEMENT. This Agreement, including all Schedules, contains all agreements of the parties. Entire agreement means State of Michigan Contract, Software Source Code Escrow Agreement, Software License Agreement, Software Maintenance Agreement and Equipment Service Agreement. No prior or contemporaneous agreement or understanding shall be effective unless specifically incorporated herein

MICHIGAN specifically acknowledges that neither Virtual Alert nor any agent or employee of Virtual Alert has made any representations, warranties or promises except as herein expressly set forth in the Agreement, including representations on any Schedule.

(b) NO WAIVER. No failure by either party to enforce any rights hereunder shall constitute a waiver of such right.

(c) NATURE OF RELATIONSHIP OF PARTIES. MICHIGAN takes no property rights at the Site. Nothing contained herein shall be deemed to create a relationship between MICHIGAN and Virtual Alert of employer and employee, master and servant, principal and agent, contractor and subcontractor, co-venturers, partners or any similar relationship within the meaning of any law or otherwise. This Agreement shall not constitute either party as the agent for or principal of the other.

(d) TARIFFS. Virtual Alert may be required to file tariffs with regulatory agencies with respect to the delivery of certain Services deemed to be telecommunications under federal or state law. If so, then to the extent such provisions are or become effective, the applicable tariff shall govern Michigan's provision of the relevant Service.

(e) SEVERABILITY. Any provision of this Agreement which shall be found to be invalid, void or illegal shall in no way affect, impair or invalidate any other provision hereof and the remaining provisions hereof shall remain in full force and effect to the greatest extent permitted by law.



(f) COUNTERPARTS. This Agreement may be executed in any number of counterparts and each such counterpart shall be deemed to be an original, but all of which, when taken together, shall constitute one agreement.

(g) APPLICABLE LAW / VENUE. Disputes related to the terms of this Agreement shall be governed by the laws of the state of Michigan, without regard to choice of law principles. .

IN WITNESS WHEREOF, the parties have caused this Equipment Location and Services Agreement to be executed as of the day and year first above written.

Virtual Alert, Inc.

("MICHIGAN")

By: _____

By: _____

Printed Name: ANDREW TRICKET

Printed Name: JIM KONRAD

Title: Chief Operating Officer

Title: Director, Tactical Purchasing

Date: _____

Date: _____

SCHEDULES

- 1 - Equipment / Services and Pricing
- 2 - MICHIGAN Equipment List



SCHEDULE 1 - Equipment / Services and Pricing

Virtual Alert Co-Location and Operations Pricing

Setup Charge			
Item	Unit	Price	Extended Price
Site Setup Charge	1	\$3,000.00	\$3,000.00
Total Setup Charges			\$3,000.00

Monthly Recurring Expenses			
Item	Unit	Price	Extended Price
Location Expense for pilot system	1	\$1,200.00	\$1,200.00
Internet Access, .5 - 2.5 Mbps Burstable, 95%*	1	\$750.00	\$750.00
Internet Access, 1.0 - 3.0 Mbps Burstable, 95%*	0	\$1,350.00	\$0.00
Internet Access, 2.0 - 10.0 Mbps Burstable, 95%*	0	\$2,700.00	\$0.00
System Services and Maintenance	1	\$2,100.00	\$2,100.00
Managed Security Devices	1	\$1,100.00	\$1,100.00
Administrative Review	1	\$1,700.00	\$1,700.00
Total Recurring Expenses			\$6,850.00

Services denoted by an asterisk "*" are invoiced based upon usage. Customer's Monthly Recurring Charge will vary depending on usage. The Monthly Recurring Charge set forth above for such usage based Service(s) is the minimum charge that may be assessed in any month.

The above quotation assumes that MICHIGAN will provide the necessary servers, the Cisco PIX 515 firewall, the Cisco 3550 Switch with Level 3 VLAN capabilities, the Uninterruptible Power Supplies, rack (if needed), rack console, KVM switch, Power Distribution Unit, Server SSL Certificate, all Microsoft Software, Trend Micro Neat Suite and Portal Protect and Veritas Backup-Exec with Portal Engine.

Installation Service

Installation service includes:

- ◆ Installing all components in rack
- ◆ Providing power to the system
- ◆ Providing the specified internet access bandwidth to the system
- ◆ Testing the firewall
- ◆ Loading and configuring certificates
- ◆ Testing the external security testing
- ◆ Loading all third party software
- ◆ Loading the Virtual Alert Software
- ◆ Loading the client's Public Health Directory information
- ◆ Testing the systems connectivity



- ◆ Providing as-built documentation of the system

Virtual Alert will provide a qualified systems engineer to perform all of these duties at our co-location facility and ensure that all activities are done completely and correctly.

Location Expense

The location expense provides for the secure facility that the system will be housed in. This facility provides the power that is needed to run the system as well as a environment control system to maintain the optimal operating parameters for the system 24 hours a day, 7 days a week. Virtual Alert staff has 24x7 access to the location and can escalate to the co-location service provider.

Internet Access

Virtual Alert will provide for Internet connectivity in a metered fashion. The quotation above is for .5Mbps nominal that is burstable to 2.5Mbps. This means that during daily use the system will be running at .5Mbps but when an event drives use of the system up the system will accommodate for the added load by broadening the potential bandwidth to 2.5Mbps. This is billed at the 95th percentile. This means that there are frequent readings of the bandwidth that is being used and the client is billed at the average load over 95% of the time. In the pilot phase of production it would be difficult for the client to overload the .5Mbps that will be available but in the event that the more bandwidth is needed the client will be billed commensurate with the load.

Virtual Alert will provide monthly usage analysis to MICHIGAN and review with your pilot team. This will provide vital feedback to the pilot process in order to assist with assessing the success of the pilot, and capacity planning for the production system.

System Services and Maintenance

Virtual Alert will monitor the applications that are used by the system to ensure that they are kept up to date and running properly. Virtual Alert will not add any update or fixes to the system without first verifying that they will not affect the system negatively by testing the updates in Virtual Alert's test environment. This will be true for all of the applications that are loaded on the system including the Virtual Alert BTRS product. There are many updates and fixes released for the applications that are used on the system but not all of them should be added without testing the updates in a similar environment before allowing them into the production environment.

Virtual Alert will backup the system once a day on an eight-week rotation. This will consist of full backups twice a week and incremental backups the other days. Further, once every rotation Virtual Alert will run a full backup that will be stored in a location other than the location that the system is located. This external backup can be used for Disaster Recovery or Operational Recovery purposes. Virtual Alert can ship tapes to MICHIGAN for a nominal extra fee.

Virtual Alert will monitor the entire system to ensure that it is constantly running at its peak performance. This will include providing reports and data to the client about the systems performance and use so that the client may identify what parts of the system are most being accessed. Further, Virtual Alert will monitor the overall health of the system



and attempt to identify potential problems before the impact the day-to-day use of the system.

Manage Security Devices

Virtual Alert will ensure that the Cisco PIX, Microsoft Internet Security and Accelerator server and Cisco 3550 VLANs are kept up to date and monitored so that they will continuously provide the highest possible level of security for MICHIGAN's pilot. When combined with the Server Certificate to enable SSL-128 bit encrypted sessions, as per CDC Guidance, this provides transport level security as be available from the SSL Certificate provider. Virtual Alert understands that the information on MICHIGAN's HAN system is potentially sensitive and thus must be protected from unauthorized intrusion. Further, the proliferation of denial of service and other attacks on systems requires that the system be prepared to automatically fend off attacks that would prevent the use of the system. Virtual Alert will monitor the security systems and prevent these attacks from having an impact on the system,

Administrative Review

Virtual Alert will provide monthly reports organized in such a way that a non-technical person can understand. The reports will cover uptime, problems encountered, enhancements made, backups executed, usage levels and other information so that the necessary people at MICHIGAN will clearly understand the health and utilization of the system.

These reports, when completed, will be posted to the system in a designated folder for easy review. Virtual Alert will also attend a conference call, if desired, with MICHIGAN to go through the individual reports.

Long Distance Charges

The above pricing does not include any charges that MICHIGAN may incur for long distance calls, caused by telephonic/fax alerts or fax distribution of documents from the BTRS portal. Such costs will be billed to MICHIGAN on a monthly basis.



SOURCE CODE LICENSE AND USE AGREEMENT

(Source-Code Released from Escrow)

THIS SOURCE CODE LICENSE AND USE AGREEMENT ("Agreement") is made and entered into as of the date the Source Code is release to Purchaser by Escrow Holder pursuant to the Source Code Escrow Agreement between the parties.(the "Effective Date"). The parties agree as follows:

1. DEFINITIONS.

1.1 "Approved CPU" means the host computer on which Purchaser is authorized to use the Software pursuant to the terms and conditions the License Agreement issued pursuant to the Purchase Agreement.

1.2 "Authorized Site" means the specific address of Purchaser's facility consisting of a single building or multiple buildings in a state or local government or municipality maintained or leased facility where the Approved CPU is physically located and operated by the Purchaser or political or governmental subdivision of Purchaser.

1.3 "Confidential Information" means: (i) the Software Source Code; (ii) the technology, ideas, know how, documentation, processes, algorithms and trade secrets embodied in the Software; (iii) any software keys related to the Software; and (iv) any other information, whether disclosed orally or in written or magnetic media, that is identified as "confidential," "proprietary" or with a similar legend at the time of such disclosure. Confidential Information shall not include any information which is: (a) published or otherwise available to the public other than by breach of this Agreement by Purchaser; (b) rightfully received by Purchaser from a third party without confidential limitations; (c) independently developed by Purchaser as evidenced by appropriate records; (d) known to Purchaser prior to its first receipt of same from Virtual Alert as evidenced by appropriate records; (e) hereinafter disclosed by Virtual Alert to a third party without restriction on disclosure; or (f) approved for public release by written authorization of Virtual Alert. If any Confidential Information must be disclosed to any third party by reason of legal, accounting or regulatory requirements beyond the reasonable control of Purchaser, Purchaser shall promptly notify Virtual Alert of the order or request and permit Virtual Alert (at its own expense) to seek an appropriate protective order.

1.4 "End User" means any department to which Purchaser has obtained licenses from Virtual Alert to use the software or such entity's own use, pursuant to a Product License Agreement.

1.5 "End User License Agreement" means a written license agreement in a commercially reasonable form containing the restrictions specified in Section 3.2, pursuant to which Purchaser may sublicense to End Users.

1.6 "Intellectual Property Rights" means all copyrights, trademarks, trade secrets, patents, mask works and other intellectual property rights recognized in any jurisdiction worldwide, including all applications and registrations with respect thereto.



- 1.7 “Object Code”** means computer-programming code in a form not readily perceivable by humans and suitable for machine execution without the intervening steps of interpretation or compilation.
- 1.8 “Permitted Modifications”** means (i) without limitation, any adaptations, modifications, improvements, enhancements, revisions or interface elements created from the Software (whether such modifications are in Object Code or Source Code) in any form or medium whatsoever; and (ii) any “derivative” work of the Software as defined in the Copyright Law of the United States of America, 17 U.S.C. §101 et seq.
- 1.9 “Project”** means a concerted undertaking by the Purchaser’s development team to repair or reproduce a Target Application that uses a specific target microprocessor and that has a specified scope of functionality, which is the same as, delivered under the Purchase Agreement.
- 1.10 “Purchase Agreement”** means the original Purchase Order as described in the Software Source Code Escrow Agreement that this Exhibit is attached and incorporated therein by reference as if fully set forth therein.
- 1.11 “Run-Time Module”** means the machine-executable object code derived from compiling the Software, any Permitted Modifications thereto, or any portion thereof, to be incorporated into a Target Application as inseparably embedded code.
- 1.12 “Software”** means (i) the computer programming code and accompanying documentation, including updates (if any), provided by Virtual Alert under the Purchase Agreement, and (ii) all Permitted Modifications thereto and full or partial copies thereof, whether such modifications or copies are provided by Virtual Alert or made by Purchaser as permitted under this Agreement.
- 1.13 “Source Code”** means computer-programming code in human readable form that is not suitable for machine execution without the intervening steps of interpretation or compilation.
- 1.14 “Target Application”** means an item, device or system originally delivered by Virtual Alert under the Purchase Agreement and installed at an Authorized Site.

2 LICENSE.

2.2 Development License. Subject to Purchaser’s compliance with the terms and conditions of this Agreement and payment under the original Purchase Agreement, Virtual Alert hereby grants to Purchaser a restricted, personal, non-transferable, non-exclusive, internal-use only license: (i) to use the Software Source Code, solely at the Authorized Site, on the Approved CPU, in connection with the repair of maintenance of the Product; (ii) to reproduce the Software Source Code for archive purposes, consistent with Purchaser’s standard archive procedures; (iii) to create Permitted Modifications of the Software Source Code, solely to the extent necessary to support the development of the Target Application; and (iv) to compile the Software Source Code and any Permitted Modifications into a Run-Time Module.

2.3 Distribution License. Subject to Purchaser’s compliance with the terms and conditions of this Agreement, Virtual Alert hereby grants to Purchaser a personal, non-



transferable, non-exclusive license: (i) to reproduce the number of copies of the Source Code, solely in machine-executable object code form, at the Authorized Site; and (ii) to distribute such copies of the Source Code to End Users within the governmental organizations that were originally licensed under the Purchase Agreement solely as inseparably embedded code in the Target Application, subject to an End User License Agreement (as defined in Section 3.2).



APPENDIX 5 SOFTWARE MAINTENANCE AGREEMENT



SOFTWARE MAINTENANCE AGREEMENT

THIS SOFTWARE MAINTENANCE AGREEMENT is entered into on this Seventeenth day of March 2003 (the "Maintenance Agreement") between Virtual Alert, Inc., a corporation existing under the laws of the State of California (hereinafter referred to as "Virtual Alert"), and State of Michigan (hereinafter referred to as "Licensee").

RECITALS

WHEREAS, Virtual Alert has developed the Bio-Terrorism Readiness Suite software ("Software") in response to the Center for Disease Control's ("CDC") Health Action Network framework;

WHEREAS, Licensee and Virtual Alert have executed the Software License Agreement for the Software; and

WHEREAS, Licensee wishes to engage Virtual Alert to perform maintenance services in connection with the Software and Virtual Alert desires to provide such maintenance services;

NOW THEREFORE, in consideration of the mutual promises and agreements set forth in this Maintenance Agreement, Virtual Alert and Licensee agree as follows:

1. Definitions. The following words shall have the following meanings when used in this Agreement:

1.1 "Affiliates" shall mean entities any departments or subdivisions that are controlled by or are under common control with Licensee.

1.2 "Bypass" shall mean a procedure communicated by Virtual Alert to Licensee, which permits Licensee to avoid Error(s) by implementing the same when using the Software.

1.3 "Enhancements" shall mean a modification to the Software that does not substantially change the functionality as described in the Functional Specifications.

1.4 "Errors" shall mean a failure of the Software to conform to the Functional Specifications.

1.5 "Error Report" shall mean the document to be created by Virtual Alert, pursuant to Article 3 hereof, each time that Licensee reports an Error.

1.6 "Fix(es)" shall mean the software and documents created by Virtual Alert pursuant to this Agreement in order to correct Errors.

1.7 "Functional Specifications" shall mean those specifications set forth Software License Agreement.

1.8 "License" shall mean the license granted by Virtual Alert to Licensee to use the Software under the Software License Agreement.

1.9 "Maintenance Representative" shall mean the person(s) appointed by Licensee at each Affiliate, provided such Affiliate uses the Software pursuant to the Software License Agreement, to work as a liaison between Virtual Alert and such Affiliate with regard to the Affiliate's Maintenance Services.

1.10 "Maintenance Services" shall mean the services to be provided under this Maintenance Agreement.



1.11 “Object Code” shall mean the binary machine readable version of the Software.

1.12 “Severity Level” shall mean the level of severity assigned to a reported Error with the Software, in accordance with the Severity Level definitions set forth in Exhibit “A” to this Agreement.

1.13 “Site” shall mean a Licensee computer facility located in one specific geographic location.

1.14 “Software” shall mean Virtual Alert’s Bio-Terrorism Readiness Suite as it complies with the Functional Specifications and shall only include the software, Bypasses, Fixes, Enhancements and Updates.

1.15 “Software Products” shall mean all physical components, other than program codes that are offered by Virtual Alert, including but not limited to, manuals, documentation, magnetic media, job aids, templates and other similar devices.

1.16 “Updates” shall mean the Software as Virtual Alert elects to provide improvements beyond the Functional Specifications, which Virtual Alert does not elect to separately price or market to its existing licensees and which are made available to the general client base of the Software.

Any capitalized terms not defined in this Agreement shall have the meaning set forth in the Software License Agreement.

2. Virtual Alert’s Obligations

2.1 In accordance with the terms of the Software License Agreement, Virtual Alert will provide, at no charge to Licensee, Error Corrections for the Software beginning when Licensee accepts the Software and continuing for the Error Correction Warranty Period specified in the relevant Purchase Order.

2.2 In consideration of Licensee’s performance hereunder, Virtual Alert shall, in addition to the other obligations imposed on Virtual Alert, hereby render the Maintenance Services pursuant to Section 3 hereof.

2.3 All Maintenance Services performed by Virtual Alert under this Maintenance Agreement shall be performed in a professional manner in accordance with industry standards. Virtual Alert does not warrant that the Maintenance Services of Software will be uninterrupted or Error-free.

2.4 The parties acknowledge and agree that, notwithstanding anything to the contrary herein contained, Virtual Alert shall not maintain the Licensee’s hardware or third-party software.

3. Maintenance Services

3.1 Licensee shall appoint a maximum of two (2) Maintenance Representatives at each Affiliate upon the Affiliate’s receipt of the Software. Such Maintenance Representatives shall thereafter receive the name(s) and telephone number(s) of Virtual Alert’s consultant(s). Licensee’s Maintenance Representatives can reach Virtual Alert’s consultant(s) between the hours of 8:00 AM and 5:00 PM, Pacific Standard Time, Monday through Friday, excluding holidays observed by Virtual Alert. Virtual Alert may reasonably choose to change the time zone while maintaining the same nominal hours, as Virtual Alert opens new customer support centers.

3.2 The Maintenance Representatives shall be responsible for providing notice to Virtual Alert’s consultant(s) of the desire for Maintenance Services. If Virtual Alert determines, after receiving such notice, that defects exist in the Software, or as a result of Error corrections or Maintenance Services, Virtual Alert shall correct any Errors in accord with this Maintenance Agreement. Virtual Alert’s consultant(s) will make the sole and final determination as to whether an Error exists and as to whether such Error is within the



scope of the Maintenance Services due Licensee hereunder. Virtual Alert does not warrant that the Maintenance Services or Software will be uninterrupted or Error free.

3.3 Maintenance Services. Virtual Alert shall correct all Errors in accordance with this Agreement and, in particular, Exhibit "A" hereto. During the term of this Agreement, Virtual Alert shall provide the following types of Maintenance Services:

3.3.1 Consultant Support. Virtual Alert shall provide consultant support as Virtual Alert determines is necessary. Such consultants shall serve as the Licensee's interface with Virtual Alert for a particular Error and shall ensure that the Error is handled in a timely manner as specified on Exhibit "A" hereto. All Errors shall be investigated and if Virtual Alert determines that the Error relates to the Software, or is directly caused by the Software, (a) an Error Report shall be opened, (b) the Error shall be assigned a Severity Level pursuant to the provisions of Exhibit "A" attached hereto, and (c) the Error shall be resolved in accordance with the procedures and processes set forth in Exhibit "A" hereto. If Virtual Alert determines that Licensee's needs under this Maintenance Agreement necessitate in-person consultant support, Virtual Alert may dispatch a consultant to the Site. All travel and expenses arising from such in-person support shall be billed to Licensee at Virtual Alert's actual cost.

3.3.2 Installation Services. Virtual Alert shall provide Licensee with assistance for the implementation or installation of Bypasses and Fixes, either by telephone or in person. Licensee's Maintenance Representatives can reach Virtual Alert's consultant(s) between the hours of 8:00 AM and 5:00 PM, Pacific Standard Time, Monday through Friday, excluding holidays observed by Virtual Alert. If Virtual Alert determines that Licensee's installation needs under this Maintenance Agreement necessitate in-person consultant support, Virtual Alert may dispatch a consultant to the Site. All travel and expenses arising from such in-person support shall be billed to Licensee at Virtual Alert's actual cost.

3.3.3 Bypasses. Virtual Alert shall provide to Licensee such Bypasses as are necessary to ensure the resolution of Errors which can be resolved by a Bypass.

3.3.4 Fixes. Virtual Alert shall provide to Licensee such Fixes as are necessary to ensure the resolution of such Errors which can be resolved by a Fix.

3.3.5 Enhancements. Virtual Alert shall provide to Licensee such Enhancements as it provides to the users for the Software from time to time. While Virtual Alert encourages Licensee's input for Enhancements, Virtual Alert retains the sole right to determine which Enhancements will be included.

3.3.6 Updates. Virtual Alert shall, as soon as they are made available, provide to Licensee such Updates as it provides to users for the Software from time to time. While Virtual Alert encourages Licensee's input for Updates, Virtual Alert retains the sole right to determine which Updates will be included.

3.3.7 Regular Activity Reports. Upon written request by Licensee, Virtual Alert shall provide: (a) a status report of Error resolution activities; and (b) a status report of all outstanding Error Reports. Such status reports shall contain Virtual Alert's tracking number, Error description, Error resolution status and a definitive resolution time frame and release number for all Errors.

3.4 Limitation on Maintenance Services. Notwithstanding any other provisions in this Maintenance Agreement, the following shall not be included in the Maintenance Services:



3.4.1 Resolution of already-existing problems with Licensee's current operating system or other applications.

3.4.2 Additions to the Functional Specifications of the Software that Virtual Alert chooses to separately price or market to its existing licensees.

3.4.3 Repair of the Software if it has been modified, changed or altered by anyone other than Virtual Alert.

3.4.4 Repair or resolution of Errors or damages to the Software caused by Licensee's hardware or software system if such hardware or software system does not meet Virtual Alert's specifications and Virtual Alert has previously notified Licensee of the deficiency.

3.4.5 Repair or resolution of Errors or damages to the Software caused by the deficient operational order of Licensee's computer hardware or an unsuitable operating environment.

3.4.6 Repair or resolution of Errors or damages to the Software resulting from Licensee's delay in notifying Virtual Alert of Errors.

3.4.7 Repair or resolution of Errors or damages to the Software resulting from Licensee's failure to provide troubleshooting information and access so that Virtual Alert can identify and address the problems.

3.4.8 Repair or resolution of Errors or damages to the Software resulting from failure by client staff to properly install the Software, including failure to follow installation procedures prescribed by Virtual Alert for Errors and Updates.

3.4.9 Repair or resolution of Errors or damages to the Software resulting from the Licensee using, or attempting to use, the Software for a purpose other than for that set forth in the Functional Specifications.

3.5 Fee for Professional Services. If Licensee desires any of the services listed in section 3.4, Licensee and Virtual Alert shall negotiate a separate agreement and separate fees for such services. If Virtual Alert incurs time and/or expense in fixing any of the Errors described in section 3.4, then Licensee will be liable for the time and/or expense at Virtual Alert's then prevailing professional services rates, and for actual expenses incurred. These fees and expenses will be paid within 45 days of receipt of the invoice for professional services. While Virtual Alert will take due care in avoiding the incurrence of such time and/or expense without first getting Licensee's prior approval, it is acknowledged by both parties that there may be some incidents in which Virtual Alert, acting in Licensee's best interest or serving an urgent need, must act proactively without first knowing whether the problem or Error falls within the Limitation on Maintenance Services set forth above.

3.6 Training Not Included. Training of users is not part of the Maintenance Services provided herein. Should Licensee desire Virtual Alert's Training Services, such services are subject to incremental fees and negotiation.

3.7 All work performed by Virtual Alert in connection with the Software and/or Maintenance Services described in this Maintenance Agreement shall be performed by Virtual Alert as an independent contractor and not as the agent or employee of Licensee. All persons furnished by Virtual Alert shall be for all purposes solely employees or agents of Virtual Alert and shall not be deemed to be employees of Licensee for any purpose whatsoever. Virtual Alert shall furnish, employ and have exclusive control of all persons to be engaged in performing Maintenance Services under this Maintenance Agreement and shall prescribe and control the means and methods of performing such Maintenance Services by providing adequate and proper supervision. Virtual Alert shall be solely responsible for compliance with all rules, laws and regulations relating to employment of labor, hours of labor, working condition, payment of wages and payment of taxes,



such as employment, social security and other payroll taxes, including applicable contributions from such persons when required by law.

4. Maintenance Fee and Expenses

4.1 Fee. Licensee will pay Virtual Alert eighteen percent (18%) of all licensing fees as set forth in the relevant Contract upon receipt of the software. Any fees due under subsequent renewals of this Maintenance Agreement are payable prior to the performance of any Maintenance Services. The same fees and terms stated in this Maintenance Agreement will apply to any subsequent renewals unless modifications are consented to in writing by both parties.

4.2 Reserved

4.3 Expenses. Licensee shall reimburse Virtual Alert for any and all reasonable travel and living expenses in accordance with State of Michigan travel regulations incurred by Virtual Alert in performing services under this Maintenance Agreement. These expenses shall be billed to Licensee, and Licensee shall pay these billings within forty-five (45) days of the date such services were rendered.

5. Term and Termination

5.1 Term. This Maintenance Agreement shall commence immediately following upon the execution of this Maintenance Agreement and continue through September 30, 2003. All terms and conditions of this Maintenance Agreement shall apply during any successive terms.

5.2 Termination:

5.2.1 Either party may terminate this Maintenance Agreement (i) immediately upon the termination or expiration of the Software License Agreement, (ii) upon expiration of the then-current term, provided at least sixty (60) days advance written notice of termination is given by either party, or (iii) upon thirty (30) days advance written notice if the other party has breached this Maintenance Agreement and has not cured such breach within such notice period. If Licensee later wishes to reinstate Maintenance Services, the reinstated Maintenance Services will be based on an annual period and Licensee shall pay Virtual Alert's then current Maintenance Services reinstatement fees in effect at the time of the reinstatement.

5.2.2 Upon 30 days written notice, this Maintenance Agreement shall be void at the option of Virtual Alert if the number of users of the Software is greater than that allowed under the Software License Agreement. Additionally, if Licensee violates the provisions of either this Maintenance Agreement or the Software License Agreement, both contracts shall be void at the option of Virtual Alert and shall have no further force or effect.

6. Warranty and Remedies

6.1 Warranties. Virtual Alert warrants that it will use reasonable efforts to perform the services to conform to generally accepted industry standards, provided that: (a) the Software has not been modified, changed, or altered by anyone other than Virtual Alert; (b) the operating environment, including both hardware and systems software, meets Virtual Alert's recommended specifications; (c) the computer hardware is in good operational order and is installed in a suitable operating environment; (d) Licensee promptly notifies Virtual Alert of its need for services; (e) Licensee provides adequate troubleshooting information and access so that Virtual Alert can identify and address the problems; (f) Licensee only uses the Software for the purposes for which it was originally sold and licensed; and (g) all fees due to Virtual Alert have been paid. THERE ARE NO OTHER WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, WITH RESPECT TO THIS MAINTENANCE AGREEMENT, AND THE SERVICES TO BE PROVIDED BY VIRTUAL ALERT UNDER IT INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.



7. Reserved

8. Licensee Support

8.1 The level of support that Virtual Alert can provide is dependent upon the cooperation of Licensee and the quantity of information that Licensee provides.

8.2 If Virtual Alert cannot reproduce a problem or if Licensee cannot successfully gather adequate troubleshooting information, Virtual Alert may need temporary login access to Licensee's computer system to identify and address the problem.

9. Licensee Responsibility

Licensee shall not distribute the Software to any third party. Licensee shall not make any modifications to the Software, unless otherwise allowed under the Software License Agreement. If Licensee is allowed to make modifications under such Software License Agreement, Virtual Alert shall not be responsible for maintaining Licensee modified portions of the Software or for maintaining portions of the Software affected by Licensee modified portions of the Software. The Licensee shall not use the Software for any purpose other than that for which it was originally licensed. Upon Licensee's prior written approval, corrections for difficulties or defects traceable to Licensee's errors or systems changes shall be billed at Virtual Alert's standard time and material charges.

10. Intellectual Property Rights

All Error Corrections, Bypasses, Enhancements, Fixes, Updates and any other work product created by Virtual Alert in connection with the Maintenance Services provided under this Maintenance Agreement ("Work Product") are and shall remain the exclusive property of Virtual Alert, regardless of whether Licensee, its employees or agents may have contributed to the conception, joined in its development, or paid Virtual Alert for the development or use of the Work Product. Such Work Product shall be considered Software, and subject to the terms and conditions contained herein and in the Software License Agreement.

11. Reserved

12. General

12.1 Gender; Number. The use herein of (i) the neuter gender includes the masculine and the feminine and (ii) the singular number includes the plural, whenever the context so requires.

12.2 Captions. Captions in this Agreement are inserted for convenience of reference only and do not define, describe or limit the scope or the intent of this Agreement or any of the terms hereof.

12.3 Entire Agreement. This Agreement and the State of Michigan Contract, Software Source Code Escrow Agreement, Software License Agreement, Software Maintenance Agreement and the Equipment Service Agreement contains the entire agreement between the parties relating to the transactions contemplated hereby and all prior or contemporaneous agreements, understandings, representations and statements, oral or written, are merged herein.

12.4 Modification. No modification, waiver, amendment, discharge or change of this Agreement shall be valid unless the same is in writing and signed by both parties.

12.5 Governing Law. This Agreement shall be construed and enforced in accordance with the laws of the State of Michigan. Venue for any dispute resolution shall be in the County of Ingham.



12.6 Time of Essence. TIME IS OF THE ESSENCE as to each and every provision of this Agreement

12.7 Assignment. Licensee may not subcontract, assign, or transfer its rights, duties or obligations under this Maintenance Agreement to any person or entity, in whole or in part, without the prior written consent of Virtual Alert.

12.8 Waiver. The waiver or failure of either party to exercise in any respect any right provided for herein shall not be deemed a waiver of any further right hereunder.

12.9 Severability. In the event any term, covenant, condition, provision or agreement herein contained is held to be invalid, void or otherwise unenforceable by any court of competent jurisdiction, the fact that such term, covenant, condition, provision or agreement is invalid, void or otherwise unenforceable shall in no way affect the validity or enforceability of any other term, covenant, condition, provision or agreement herein contained.

12.10 Force Majeure. Neither party shall be responsible of any delay or failure in performance of any part of this Maintenance Agreement to the extent that such delay or failure is caused by fire, flood, explosion, war embargo, government requirement, civil or military authority, act of God, act of omission of carriers or other similar causes beyond its control. If any such an event of force majeure occurs and such event continues for ninety (90) days or more, the party delayed or unable to perform shall give immediate notice to the other party, and the party affected by the other's delay or inability to perform may elect at its sole discretion to: (a) terminate this Maintenance Agreement or the affected order solely upon mutual agreement of the parties; (b) suspend such order for the duration of the condition and obtain or sell elsewhere, Software, Software Products or Maintenance Services comparable to the Software, Software Products or Maintenance Services to have been obtained under the order; or (c) resume performance of such order once the condition ceases with the option of the affected party to extend the periods of this Maintenance Agreement up to the length of time the condition endured. Unless written notice is given within thirty (30) days after the affected party is notified of the condition, option (c) shall be deemed selected.

12.11 Notice. All notices, demands or other communications herein provided to be given or that may be given by any party to the other shall be deemed to have been duly given when made in writing and delivered in person, or upon receipt, if (a) deposited in the United States mail, postage prepaid, certified mail, return receipt requested, or (b) sent by reputable overnight courier addressed as follows:



To Virtual Alert: Virtual Alert, Inc.
 Andrew Tricket
 Chief Operating Officer
Phone: (512) 732-1214
Fax: (512) 732-1202

To: Licensee: State of Michigan
 Jim Konrad, Director
 Tactical Purchasing Division
Phone: (517) 373-0315
Fax: (517) 335-0046

12.12 Survival of Clauses. Sections 6, 7, 9 and 10 shall survive termination of this Maintenance Agreement.

12.13 Export Regulations. Licensee and Virtual Alert acknowledge that the Software and all related technical information, documents and materials may be subject to export controls under the U.S. Export Administration Regulations, and to the extent applicable, Licensee and Virtual Alert shall (a) comply with all requirements set forth in such regulations, and (b) cooperate fully with each other in any official or unofficial audit or inspection that relates to such export requirements.

12.14 Counterparts. This Agreement may be signed in one or more counterparts, each of which will be deemed to be an original and all of which when taken together will constitute the same agreement.

12.15 Conflict in the Documents. If any provision(s) of this Agreement conflict(s) with the terms of the State of Michigan Contractual Service Terms and Conditions attached hereto, then the State of Michigan Contractual Service Terms and Conditions shall be controlling

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]



IN WITNESS WHEREOF, the parties have caused this Agreement to be duly executed and delivered on the day and year first above written.

ACCEPTED AND AGREED TO:

VIRTUAL ALERT, INC.

By: _____
Andrew Tricket

Title: Chief Operating Officer

ACCEPTED AND AGREED TO:

LICENSEE

By: _____
Jim Konrad

Title: Director, Tactical Purchasing Division
State of Michigan



EXHIBIT A

Maintenance Response Schedule

1. Virtual Alert's consultant(s) shall return calls within the time specified in the Response Schedule set out below. Such response times shall be measured from the time a Licensee Contact requests support by one of the means set forth below.

2. Licensee's Support Representatives shall report errors and defects to Virtual Alert to one of the consultants designated by Virtual Alert. For Severity 1 errors or defects, Licensee's Support Representatives shall in addition to any notification by any other means, notify Virtual Alert by telephoning a consultant. In the event Licensee cannot make contact with a Virtual Alert consultant, Licensee shall continue its efforts to personally notify Virtual Alert by calling the following Virtual Alert representatives in the order listed until a Virtual Alert Representative is contacted in person.

- i Licensee Service Manager
- ii Chief Operating Officer
- iii Chief Technology Officer
- iv Chief Executive Officer

3. Licensee will make an initial nonbinding classification of each Error or defect with the Software or Support Materials and will report such Error or defect to Virtual Alert based on the criteria set forth below. In the event there is a dispute between the Licensee and Virtual Alert regarding the classification of such Error or defect that is not resolved within 24 hours after the report from Licensee, such dispute shall be referred to Virtual Alert's Director-level management for resolution. Virtual Alert retains the sole right to make the final determination as to the classification of such problem.

Error Classification Criteria

- Severity Level 1 Critical Business Impact
- Severity Level 2 Significant Business Impact
- Severity Level 3 Non-Critical
- Severity Level 4 Minimal Impact

4. In the event Licensee reports a problem to Virtual Alert during Virtual Alert's normal business hours, Virtual Alert shall use commercially reasonable efforts to respond to such reports in accordance with the following Software Maintenance Response Schedule.



Software Maintenance Response Schedule

Error Classification	1 st Level	2 nd Level	3 rd Level
Severity 1	1 business hour	4 business hours	Next Release
Severity 2	2 business hours	1 business day	Next Release
Severity 3	2 business days	To be scheduled as appropriate	
Severity 4	7 business days	To be scheduled as appropriate	

Level Identification

Level 1: Acknowledgement of receipt and Error report

Level 2: Commencement of patch, work around, temporary fix, Bypass and other temporary resolution of the Error and documentation of corrections.

Level 3: Official Object Code fix incorporated in a Fix, Enhancement or Update to the Software.

“To be scheduled” means that the parties shall address the Error at the next scheduled project review meeting and in good faith agree on a suitable Level 2 response.

“Next Release” means the release of a Fix, Enhancement or Update to the Software that corrects Errors and defects or makes minor improvements in the functionality of the Software which is generally made available to Virtual Alert’s client base.

5. Licensee must supply Virtual Alert with reproducible Errors in order for the Response Schedule to apply. The manner in which Licensee reasonably presents to Virtual Alert the method or means to reproduce such a reported Error is up to Licensee. For non-reproducible Errors except for a Severity 1 Error, Virtual Alert will use reasonable efforts to investigate the Error, but shall not be bound by the above schedule. In the event Licensee cannot reproduce a Severity 1 Error despite Licensee’s best efforts, Virtual Alert shall be required to comply with the 1st and 2nd level response times as set forth above, but Virtual Alert shall not be obligated to provide personnel to work on the Error if the Error has not been replicated within 48 hours from the time that Virtual Alert began working with Licensee. For any period of time in which Virtual Alert has assigned personnel to address a non-reproducible Error, Licensee agrees to assign no fewer development personnel than that which Virtual Alert has assigned, and Licensee agrees that such personnel shall work no fewer hours than that worked by Virtual Alert personnel in addressing the problem. Should the parties later discover that the Services provided to address the non-reproducible Error was not within the scope of the Maintenance Services in the Maintenance Agreement or should Licensee fail to staff the situation as described in the preceding sentence, Licensee shall pay Virtual Alert for all professional time (at Virtual Alert’s then-current rates) and related expenses incurred by Virtual Alert in response to such Error.



APPENDIX 6
Three-Party Escrow Agreement
Among
Developer, one Licensee and Escrow Associates, LLC



Three-Party Escrow Agreement

Among

Developer, one Licensee and Escrow Associates, LLC

This three-party agreement allows the software licensee conditional access to the source code. The Licensee, Software Developer and Escrow Associates, LLC all execute the agreement.



Three-Party Escrow Agreement

This Technology Escrow Agreement ("Agreement") among Escrow Associates, LLC ("Escrow Associates"), the State of Michigan ("Licensee") and Virtual Alert, Inc. ("Developer") is effective on this Seventeenth day of March 2003 (the "Effective Date").

Recitals

Whereas, Developer licenses technology to Licensee in the form of software object code (the "Software") pursuant to a license agreement ("License Agreement"). The source code is defined as the Software in source code form, including all relevant documentation and instructions necessary to maintain, duplicate, and compile the source code (the "Source Code"). The Source Code is necessary to maintain and support the Software as defined in the License Agreement. The Source Code and any other components Developer provides which are related to building and maintaining the Software identified on Exhibit B (as the same may be modified herein) are hereafter referred to collectively as the deposit materials ("Deposit Materials").

Whereas, the purpose of this Agreement is to protect Developer's ownership and confidentiality of the Deposit Materials and to protect Licensee's legitimate use of the Deposit Materials as defined by the License Agreement. Further, this Agreement is intended to provide for certain circumstances under which the Licensee shall be entitled to receive the Deposit Materials held in escrow by Escrow Associates to continue its legitimate use and support of the Software.

Whereas, the Licensee and Developer hereby designate and appoint Escrow Associates as the escrow agent under this Agreement. Escrow Associates hereby accepts such designation and appointment and agrees to carry out the duties of escrow agent pursuant to the terms and provisions of this Agreement. Escrow Associates is not a party to, and is not bound by, any agreement that might be evidenced by, or might arise out of, any prior or contemporaneous dealings between Developer and Licensee other than as expressly set forth herein.

Whereas, the parties desire that this Agreement be an agreement supplementary (together with any modification, supplement, or replacement thereof agreed to by the parties) to the License Agreement pursuant to Title 11 United States Bankruptcy Code Section 365(n).

NOW, THEREFORE, for and in consideration of good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereto, intending to be legally bound hereby, covenant and agree as follows:

1. Deposit Materials

(a) Initial Deposit - Developer shall submit the initial Deposit Materials to Escrow Associates within sixty (60) days of the Effective Date or sixty (60) days after development of the Deposit Materials is completed. Developer shall complete and deliver with all Deposit Materials a form as shown herein as Exhibit B, which shall then become part of this Agreement. Escrow Associates shall notify Licensee within ten (10) days of receipt of the initial Deposit Materials. Escrow Associates has no obligation with respect to the initial Deposit Materials for delivery, functionality, completeness, performance or initial quality.



(b) Deposit Material Updates - Developer shall submit updates to the initial Deposit Materials to Escrow Associates within sixty (60) days of any material modification, upgrade or new release of the Software. Developer shall complete and deliver with all updates to the Deposit Materials an amended Exhibit B form, which shall additionally become part of this Agreement. Escrow Associates shall notify Licensee within ten (10) days of receipt of updates to the Deposit Materials. Escrow Associates has no obligation with respect to the updates to the Deposit Materials for delivery, functionality, completeness, performance or initial quality.

(c) Electronic Deposit – In the event the Developer elects to utilize electronic means to transfer the Deposit Materials to Escrow Associates, whether through a service provided by Escrow Associates or other means, Escrow Associates shall not be liable for transmissions that fail in part or in whole, are lost, or are otherwise compromised during transmission. Furthermore, Escrow Associates shall not be liable for any subsequent services that may or may not be delivered as a result of a failed transfer. Escrow Associates shall not be liable to Developer or Licensee for any encrypted update, or any part thereof, that is transmitted over the Internet to Escrow Associates' FTP Site but is not received in whole or in part, or for which no notification of receipt is given.

(d) Duplication of Deposit Materials - Escrow Associates may duplicate the Deposit Materials only as necessary to comply with the terms of this Agreement. Escrow Associates at its sole discretion may retain a third party for the purpose of duplicating the Deposit Materials only as necessary to comply with the terms herein. All duplication expenses shall be borne by the party requesting duplication.

(e) Deposit Material Verification - Escrow Associates may be retained by separate agreement or by alternative means, to conduct a test of the Deposit Materials to determine the completeness and accuracy of the Deposit Materials. Escrow Associates shall not be liable for any actions taken on the part of any third party with regards to the Deposit Materials.

2. Term

(a) Term of Agreement – The term of this Agreement shall be for a period through September 30, 2003. At the end of the initial and each subsequent term, this Agreement shall automatically renew for an additional one (1) year term unless terminated according to the terms herein.

(b) Termination of Agreement – This Agreement may be terminated by written mutual consent of the Developer and Licensee provided that one of the following occurs:

- i. The License Agreement has been terminated or has expired, or
- ii. The Deposit Materials have been released in accordance with the terms hereof.

(c) Termination for Non-Payment – Virtual Alert, Inc. is responsible to pay any or all fees due to Escrow Associates under this Agreement. In the event that full payment of any or all fees due to Escrow Associates under this Agreement have not been received by Escrow Associates within thirty (30) days of the date payment is due, Escrow Associates will notify all parties hereto of the delinquent fees. If the delinquent fees are not received within thirty (30) days of the delinquency notification, Escrow Associates shall have the right to terminate this Agreement.



(d) Return of Deposit Materials – Upon termination of this Agreement for any reason other than in the event all Deposit Materials have been released, Escrow Associates shall return the Deposit Materials to the Developer via commercial courier to the address of the Developer shown in this Agreement, provided that all fees due Escrow Associates are paid in full. If two (2) attempts to return Deposit Materials via commercial courier to the Developer fail or the Developer does not accept the Deposit Materials, Escrow Associates shall destroy the Deposit Materials.

3. Fees

(a) Payment - Upon receipt of signed Agreement or initial Deposit Materials, whichever comes first, Escrow Associates will submit an initial invoice to Developer for amount shown on Exhibit A attached hereto. If payment is not received, Escrow Associates shall have no obligation to perform its duties under this Agreement. Developer agree to pay to Escrow Associates all additional fees for services rendered related to this Agreement as shown on Exhibit A. The fee for any service that is not expressly covered in Exhibit A shall be established by Escrow Associates upon request. All fees are due in advance of service and are non-refundable. Escrow Associates may amend Exhibit A at any time upon sixty (60) days written notice to Developer.

(b) Currency - All fees are in U.S. dollars and payment must be rendered in U.S. dollars unless otherwise agreed to in advance by Escrow Associates.

4. Indemnification - With the exception of gross negligence, willful misconduct or intentional misrepresentation on behalf of Escrow Associates, and Developer shall, jointly and severally, indemnify and hold harmless Escrow Associates and each of its directors, officers, agents, employees, members and stockholders ("Escrow Associates Indemnities") absolutely and forever, from and against any and all claims, actions, damages, suits, liabilities, obligations, costs, fees, charges, and any other expenses whatsoever, including reasonable attorneys' fees and costs, that may be asserted against any Escrow Associates Indemnatee in connection with this Agreement or the performance of Escrow Associates or any Escrow Associates Indemnatee hereunder.

5. Developer's Representations and Warranties

(a) The Deposit Materials as delivered to Escrow Associates are a copy of Developer's proprietary information corresponding to that described in Exhibit B and are capable of being used to generate the Software. Developer shall update the Deposit Materials as provided for in the License Agreement and/ or as provided for herein. The Deposit Materials shall contain all information necessary to enable a reasonably skilled programmer or analyst to understand, maintain and correct the Deposit Materials.

(b) Developer owns the Deposit Materials and all intellectual property rights therein free and clear of any liens, security interests, or other encumbrances.



6. Release of Deposit Materials

(a) Release - The Deposit Materials, including any copies thereof, will be released to the Licensee after the receipt of the written request for release only in the event that the release procedure set forth in Section 6 is followed and:

- i. Developer notifies Escrow Associates in writing to effect such release; or
- ii. Licensee makes written request to Escrow Associates; and
 - a. Licensee asserts that Developer has failed in a material respect under the License Agreement; and
 - b. Licensee includes a written statement that the Deposit Materials will be used in accordance with the terms of the License Agreement; and
 - c. Licensee includes specific instructions for the delivery of the Deposit Materials.

(b) Developer Request for Release - If the provisions of Section 6(a)(i) are met, Escrow Associates will release the Deposit Materials to Licensee within ten (10) business days.

(c) Licensee Request for Release - If the provisions of Section 6(a)(ii) are met, Escrow Associates will within ten (10) business days forward a complete copy of the request to Developer. Developer shall have fifteen (15) to make any and all objections to the release known to Escrow Associates in writing. If after fifteen (15) days Escrow Associates has not received any written objection from Developer, Escrow Associates shall release the Deposit Materials to the Licensee as instructed by the Licensee.

(d) Developer Objection to Release - Should the Developer object to the request for release by Licensee in writing, Escrow Associates shall notify the Licensee in writing within ten (10) business days of Escrow Associates receipt of said objection and shall notify both parties that there is a dispute to be resolved pursuant to Section 7 (Arbitration) of this Agreement. Escrow Associates will continue to hold the Deposit Materials without release pending (a) joint instructions from Developer and Licensee; (b) dispute resolution according to Section 7 (Arbitration); or (c) order from a court of competent jurisdiction.

(e) Right to Use Following Release - Unless otherwise provided in the License Agreement, upon release of the Deposit Materials in accordance with this Section 6, Licensee shall have the right to use the Deposit Materials for the sole purpose of continuing to support its licensed usage afforded to Licensee by the License Agreement. Licensee shall be obligated to maintain the confidentiality of the released Deposit Materials. Any and all modifications or derivative works created through use of the Deposit Materials shall be deemed as the Software governed by the terms of the License Agreement.

7. Reserved.

8. Confidentiality – Except as otherwise required to carry out its duties under this Agreement, Escrow Associates shall hold in strictest confidence and not permit any third party access to nor otherwise use, disclose, transfer or make available the Deposit Materials except as otherwise provided herein, unless consented to in writing by Developer.

9. Limitation of Liability - Under no circumstance shall Escrow Associates be liable for any special, incidental, or consequential damages (including lost profits) arising out of this Agreement even if Escrow Associates has been apprised of the possibility of such damages. In performing any of its



duties hereunder, Escrow Associates shall not incur any liability to any party for any damages, losses, or expenses, except for willful misconduct or gross negligence on the part of Escrow Associates, and it shall not incur any liability with respect to any action taken or omitted in reliance upon any written notice, request, waiver, consent, receipt or other document which Escrow Associates in reasonably good faith believes to be genuine.

10. Notices – Notices shall be deemed received on the third business day after being sent by first class mail, or on the following day if sent by commercial express mail. All notices under this Agreement shall be in writing and addressed and sent to the person(s) listed in the space provided below:

Developer

Company: _ Virtual Alert, Inc.
 Contact: Andrew Trickett; Title: Chief Operating Officer
 Address: 7000 Bees Caves Road #300
 City, State, Zip: Austin, TX 78746
 Telephone: (512) 732-1214
 Fax: (916) 565-4294
 Email:

Billing Contact: Chris Popov
 Title: Director, Business Development
 Address: P.O. Box 2985
 City, State, Zip: La Jolla, CA 92038
 Telephone: 858-775-9444

Licensee

Company: The State of Michigan, Acquisition Services
 Contact: Jim Konrad Title: Director,
 Tactical Purchasing
 Address: 530 West Allegan, Mason Bldg., 2nd floor
 City, State, Zip: Lansing, MI 48909
 Telephone: 517-335-0230
 Fax: 517-335-0046
 Email: konradj@michigan.gov

Escrow Associates

Attn: Contracts Administration
 1010 Huntcliff, Suite 1350
 Atlanta, GA 30350 USA
 Telephone: 800-813-3523
 Fax: 770-518-2452
 Email: info@escrowassociates.com



11. Miscellaneous

(a) Counterparts - This Agreement may be executed in any number of multiple counterparts, each of which is to be deemed an original, and all of such counterparts together shall constitute one and the same instrument.

(b) Entire Agreement - This Agreement supersedes all prior and contemporaneous letters, correspondences, discussions and agreements among the parties with respect to all matters contained herein, and it constitutes the sole and entire agreement among them with respect thereto.

(c) Limitation of Effect - This Agreement pertains strictly to the escrow services provided for herein and does not modify, amend or affect any other contract or agreement of one or more of the parties. The terms and provisions of the License Agreement, as the same may be physically modified by the terms and provisions hereof, shall continue in full force and effect and be binding upon and inure to the benefit of the parties hereto, their legal representatives, successors and assigns.

(d) Modification - This Agreement shall not be altered or modified without the express written consent of all parties.

(e) Bankruptcy Code - This Agreement shall be considered an agreement supplementary (together with any modification, supplement, or replacement thereof agreed to by the parties) to the License Agreement pursuant to Title 11 United States Bankruptcy Code Section 365(n).

(f) Survival of Terms - All obligations of the parties intended to survive the termination of this Agreement, including without limitation, are the provisions of paragraphs 2 (Term), 3 (Fees), 4 (Indemnification), 9 (Limitation of Liability), and 11 (Miscellaneous) which shall survive the termination of this Agreement for any reason.

(g) Governing Law - This Agreement shall be governed by the laws of the state of Michigan.

(h) Time of the Essence - Time is of the essence in this Agreement.

(i) Successors and Assigns - This Agreement shall be binding upon and inure to the benefit of the successors and assigns of the parties, provided, however, that Licensee shall have no right to assign any rights hereunder or with respect to the Deposit Materials except as permitted with respect to assignment of Licensee's rights under the License Agreement.

(Signatures are on following page. Remainder of the page intentionally left blank.)



IN WITNESS WHEREOF, the parties have executed this Agreement by and through their duly authorized agents as of the Effective Date.

Developer

Signature: _____

Name: **Andrew Trickett**

Title: **Chief Operating Officer**

Company: **Virtual Alert Inc.**

Date: _____

Telephone: (512)-732-1214

Licensee

Signature: _____

Name: **Jim Konrad**

Title: **Director, Tactical Purchasing**

Company: **State of Michigan**

Date: _____

Telephone: (517) 335-0230

Escrow Associates, LLC

Signature: _____

Name: **Christian Dodder**

Title: Account Executive

Date: _____

Exhibit A
Schedule of Fees

Initialization Fee	\$ 900
(First-year fee only. Includes all contract review, modification and set-up of account.)	
Annual Maintenance Fee	\$ 1200
(Annual fee. Includes escrow deposit maintenance, all account activity notifications, unlimited escrow deposit material updates, online account information access, electronic depositing option, and two (2) cubic ft. storage allowance.)	

Additional Items Menu

Additional Storage Space	\$ 100/ cubic ft.
Deposit Material Reporting	\$ 600 annually
Technical Verification	Contact Us



Exhibit B
Deposit Materials

Please complete an Exhibit B document for the Deposit Materials to be escrowed under this account. Enclose a copy of this Exhibit B with the Deposit Materials and retain a copy for your records. Ship the Deposit Materials to Escrow Associates at the following address:

Attn: Vault Manager
Escrow Associates, LLC
1010 Huntcliff, Suite 1350
Atlanta, GA 30350 USA
1-800-813-3523

Company Name: _____

Product Name & Version: _____

Media Description

Quantity	Type	Description / Label
_____	CD-ROM	_____
_____	DAT/DDS Tape	_____
_____	Documentation	_____
_____	Other	_____

Deposit Prepared by: _____

Date: _____

E-mail: _____

Escrow Associates has inspected and accepted the above Deposit Materials.

Signed: _____

Name: _____

Date: _____